

September 22, 2021

Erratum

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Re: ET Docket No. 21-232, *Protecting Against National Security Threats to the
Communications Supply Chain through the Equipment Authorization Program*

Dear Ms. Dortch:

On September 20, 2021, Hikvision USA, Inc. (“Hikvision”) filed comments with the Commission on the Commission’s Notice of Proposed Rulemaking proposing to prohibit further authorization of equipment on the Covered List. The attached comments correct an error which was the result of a conforming change being inadvertently omitted. Hikvision submits this erratum to request that the Commission substitute the attached comments for the version filed on September 20.

Sincerely,



John T. Nakahata
Counsel to Hikvision

Corrected
Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of

Protecting Against National Security Threats to
the Communications Supply Chain through the
Equipment Authorization Program

ET Docket No. 21-232

COMMENTS OF HIKVISION USA, INC.

John T. Nakahata
Timothy J. Simeone
Deepika Ravi
John Grimm
Annick Banoun
HARRIS, WILTSHIRE & GRANNIS LLP
1919 M Street, NW, Suite 800
Washington, DC 20036
(202) 730-1300
jnakahata@hwglaw.com

Counsel for Hikvision USA, Inc.

September 20, 2021

EXECUTIVE SUMMARY

Hikvision USA, Inc. (“Hikvision”), a subsidiary of Hangzhou Hikvision Digital Technology Co., Ltd., provides these comments on the Commission’s Notice of Proposed Rulemaking (“NPRM”) proposing to prohibit further authorization of equipment on the Covered List.

Hikvision supports the Commission’s goal of protecting communications networks, consumers, and businesses in the United States from security risks; it dedicates substantial resources to the security of its products, its partners, and its end users in the United States and around the world. But the Commission’s proposal to bar Hikvision equipment from U.S. markets will not enhance national security or end-user cybersecurity. Hikvision does not provide network equipment and thus cannot divert communications or otherwise subvert communications networks. Hikvision primarily provides peripheral devices—principally cameras and associated video processors called “network video recorders”—that American companies use to protect their personnel and property. Like most networkable devices, Hikvision equipment not only has extensive security features built in, but also operates within internal company systems that end users’ IT departments design to be secure. No purpose is served by singling out Hikvision cameras and equipment for treatment different from that afforded other equipment—whether security equipment or other networkable devices—with equivalent or greater vulnerabilities.

The Commission has also failed to identify any source of legal authority permitting it to adopt the proposed ban. Under Title I, the Commission has long *disclaimed* authority to regulate peripheral devices or customer premises equipment like the equipment Hikvision sells, and the NPRM provides no basis on which to abandon that position. And while the Commission certainly has authority under section 302 of the Communications Act to regulate the RF spectrum

and interference, the NPRM's proposals have nothing to do with either. Furthermore, neither Section 889 of the National Defense Authorization Act ("NDAA") nor the Secure Networks Act ("SNA")—upon which the Commission also purports to rely—confers *any* additional authority on the Commission to regulate equipment that is not funded by USF or purchased by government agencies. In fact, in the NDAA and the SNA, Congress made the determination to restrict *only* government funding or use of Hikvision equipment for specific places and purposes, and the proposals of the NPRM therefore contradict congressional intent. Finally, the NPRM's proposals also exceed the Commission's ancillary jurisdiction. The Commission can satisfy neither the requirement of general regulatory jurisdiction under Title I, nor that of a specific statutory provision that the proposed regulations are *reasonably* ancillary to effectuating.

The proposals of the NPRM are also unlawful because they would arbitrarily and capriciously treat similarly situated parties differently. Here, the Commission appears to propose targeting individual companies on the basis of highly speculative, unsubstantiated security concerns rather than demonstrated, or even reasonably plausible, problems. Inclusion of Hikvision equipment in the "Covered List" is not a sufficient ground on which to ban such equipment altogether because, as further discussed below, the "Covered List" was created by the Congress and the Commission for a much narrower purpose and more targeted set of situations than is now proposed. Moreover, the Commission identifies no evidence whatsoever suggesting that Hikvision equipment is *more* vulnerable than that of other manufacturers across the wide range of business installations. Finally—and for similar reasons—the proposals of the NPRM are also inconsistent with the constitutional guarantee of Equal Protection. Those proposals unlawfully single out Hikvision for unequal treatment because it is Chinese, and fail even rational basis review because they are based on *irrational* logical leaps.

Table of Contents

I.	INTRODUCTION AND SUMMARY	1
II.	FACTUAL BACKGROUND	7
A.	The Equipment that Hikvision Imports into the United States Does Not— and in Many Common Installations Cannot Possibly—Pose a National Security Risk to the American Public.	7
B.	Hikvision Is a Globally Respected Video Surveillance Company.	15
C.	Hikvision Products Are Not Sold Directly to American Consumers.	16
D.	Only a Limited Number of Hikvision Product Models Are Sold in the United States, and Those Products Undergo Extensive Software Testing and Mostly Do Not Require Network Connectivity.	16
	1. Hik-Connect and HikCentral	17
	2. Software	19
E.	The Interoperability of Hikvision Equipment Is a Defense Against Potential Cyberattacks.	22
F.	Cybersecurity Is of Paramount Importance to Hikvision.	22
G.	Hikvision Empowers End Users to Implement Cybersecurity Measures to Protect Against Inbound Attacks and Outbound Transmission.	26
III.	THE COMMISSION LACKS ANY EXPRESS OR ANCILLARY AUTHORITY TO ADOPT THE PROPOSALS OF THE NPRM.	27
A.	Title III Provides the Commission Authority to Manage the RF Spectrum and Potential Interference, but No General Authority to Regulate on Public Interest or National Security Grounds.	27
B.	The Proposals of the NPRM are Inconsistent with Section 889 of the NDAA and the Secure Networks Act.	33
C.	Title I Provides the Commission Neither Direct nor Ancillary Authority Over Devices like Hikvision Cameras and NVRs that Are Peripheral to the Communications Infrastructure.	39
D.	The Commission’s General Jurisdictional Grant Under Title I Provides No Authority to Regulate Customer Premises Equipment that Is Peripheral to Communications Networks.	40

E.	The NPRM’s Proposed Ban on Hikvision Equipment Is Not “Reasonably Ancillary” to the Commission’s Effective Performance of Any Statutorily Mandated Responsibility.	45
1.	The Secure Networks Act provides no ancillary jurisdiction.	45
2.	Section 302, section 303, and other statutory provisions imposing responsibilities relating to RF spectrum and interference provide no ancillary jurisdiction under Title I.	49
3.	CALEA provides no ancillary jurisdiction.	50
IV.	THE PROPOSED REGULATIONS WOULD BE ARBITRARY AND CAPRICIOUS.....	51
A.	The Proposed Regulations Are Arbitrary and Capricious Because They Would Treat Similar Companies and Products Differently.....	52
B.	The Commission Relies on Factors Congress Did Not Intend It to Consider When Setting Equipment Authorization Criteria and Fails to Consider Less Restrictive Alternatives.....	54
C.	The Proposed Regulations Are Arbitrary and Capricious Because They Address Highly Speculative, Unsubstantiated Security Risks, not Demonstrated Problems.....	55
D.	The Proposed Regulations Are Arbitrary and Capricious Because of the Highly Disruptive Effect They Would Have on American Businesses, Consumers, and Manufacturers Globally.	61
V.	THE PROPOSED REGULATIONS WOULD VIOLATE THE CONSTITUTION’S EQUAL PROTECTION GUARANTEE.....	65
A.	The Commission’s Proposal Targets Manufacturers for Disparate Treatment Because of Their National Origin.....	65
B.	The Commission’s Regulations Cannot Survive Even Rational Basis Review, Because They Are Based on Irrational Logical Leaps.	70
VI.	THE COMMISSION’S STRUCTURE MAY VIOLATE THE APPOINTMENTS CLAUSE.....	71
VII.	CONCLUSION.....	72

I. INTRODUCTION AND SUMMARY

Hikvision USA, Inc. (“Hikvision”), a subsidiary of Hangzhou Hikvision Digital Technology Co., Ltd., provides these comments on the Commission’s Notice of Proposed Rulemaking (“NPRM”) and Notice of Inquiry proposing to prohibit authorization of equipment on the Covered List.¹

Hikvision supports the Commission’s goal of protecting communications networks, consumers, and businesses in the United States from security risks; indeed, Hikvision has dedicated substantial resources to both ensuring the security of its products and helping to provide its United States end users, partners, and distributors the information they need to keep their systems safe.² But the Commission’s proposal to bar future—and potentially even past—authorizations of Hikvision equipment will not enhance national security or end-user cybersecurity. Hikvision does not provide network equipment, and thus cannot divert communications or otherwise subvert the United States’ communications network. Hikvision provides devices—principally cameras and associated video processors called “network video recorders” (“NVRs”)—that American companies use to protect their personnel and property. Banning that Hikvision equipment will directly harm American businesses by denying them the equipment they have chosen as the best to secure their premises in a cost-effective manner. Far-fetched fears of espionage—utterly unsupported by evidence—cannot justify that harm, and such

¹ *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Notice of Proposed Rulemaking and Notice of Inquiry, FCC No. 21-73, ET Docket No. 21-232 (June 17, 2021) (“*Covered Equipment NPRM*”).

² See generally Cybersecurity Center, Hikvision, <https://us.hikvision.com/en/support-resources/cybersecurity-center> (last visited Sept. 18, 2021).

malicious conduct would in any event be readily blocked by end users employing standard cybersecurity practices.

The Commission, moreover, simply lacks authority to adopt its proposed rule. The Commission's jurisdiction over equipment authorization permits it to address potential radio frequency ("RF") spectrum interference from devices. But that jurisdiction provides no general "public interest" authority to adopt a broad importation or use ban. Congress has, moreover, conferred no other express or ancillary jurisdiction to adopt such a ban and, in fact, the Commission's proposals here are inconsistent with Congress's own determination, echoed in the Commission's Covered Entity List, *not* to ban Hikvision products generally, but rather to prohibit only specific uses.

* * *

Hikvision is one of many companies offering security cameras, video storage devices, and related security products in the United States. Hikvision does not dominate the provision of video security devices; an independent entity estimated Hikvision's U.S. market share as under 15 percent.³ In the U.S., Hikvision offers its security equipment through distribution partners marketing primarily to small- and medium-sized businesses. End users, not Hikvision, determine where and how to install their security systems. As a practical matter, many are installed either on standalone internal networks that are not connected to the Internet at all, or on virtual private networks ("VPNs") that are logically separate from other local area networks ("LANs") or wide area networks ("WANs"). Moreover, Hikvision cameras and video servers

³ Mordor Intelligence, *United States Video Surveillance Market 2021-2026*, at 164 (2020) ("Mordor Report").

are broadly interoperable with other manufacturers' hardware and software, so an end user does not have to use all Hikvision equipment.

Like other companies' video surveillance equipment, Hikvision devices are plainly not part of the core telecommunications or Internet infrastructure, but are instead "peripheral" devices of the sort the Commission has long declined to regulate. Indeed, Hikvision products are not even "communications equipment" within the meaning of the Secure Networks Act ("SNA") because they are not "essential to the provision of advanced communications service."⁴ Nor are Hikvision cameras or recorders generally "capable of routing or redirecting user data traffic or permitting visibility into any user data" within the meaning of the SNA.⁵ Like a telephone, cameras merely generate the data that is routed, if at all, by other devices in the end user's network, which the end user controls.

For reasons both practical and legal, it makes no sense for the Commission to reverse its longstanding deregulatory policy with respect to end-user devices to effectively ban the importation and sale of Hikvision equipment as proposed in the NPRM. Perhaps most fundamentally, with respect to security threats, Hikvision equipment does not raise any security issue distinct from those posed by a myriad of other networkable devices.

Moreover, like other networkable devices, Hikvision equipment not only has extensive security features built in, but also operates within internal company systems that end users' IT departments design to be secure. As noted above, cameras and video recorders frequently function as standalone, physically separate networks not linked to any WAN. Moreover, for an end user particularly concerned about cybersecurity, Hikvision equipment may be installed with

⁴ 47 U.S.C. § 1608(4).

⁵ 47 U.S.C. § 1601(b)(2)(A).

interoperable surveillance equipment from other manufacturers, further enhancing security because inbound threats would need to penetrate cybersecurity defenses of other manufacturers as well as Hikvision's—in addition to the security of the end user's own internal network. In short, no purpose is served by singling out Hikvision cameras and equipment for treatment different from that afforded other equipment—whether security equipment or other networkable devices—with equivalent or greater vulnerabilities.

As a legal matter, it is arbitrary and capricious to treat similarly situated parties differently. Here, the Commission appears to propose targeting individual companies on the basis of highly speculative, unsubstantiated security concerns rather than demonstrated, or even reasonably plausible, problems. Inclusion of Hikvision equipment in the “Covered List” is not a sufficient ground on which to ban such equipment altogether because, as further discussed below, the “Covered List” was created by the Congress and the Commission for a much narrower purpose and more targeted set of situations than is now proposed. Moreover, Hikvision has a stellar record of identifying and addressing security vulnerabilities in a transparent manner, and of pursuing and obtaining high-level security certifications for its devices. The Commission identifies no evidence whatsoever suggesting that Hikvision equipment is *more* vulnerable than that of other manufacturers across the wide range of business installations. Hikvision also takes seriously its responsibility to serve as a cybersecurity resource for its partners and end users, investing extensively in developing an array of scanning tools, unknown-vulnerability discovery tools, and network security hardening resources and best practices to help safeguard end users' systems. The Commission has pointed to no evidence that these cooperative efforts of Hikvision, its dealers, and its end users have proved in any way inadequate to address security threats to systems incorporating Hikvision equipment, to the extent that any such threats exist.

For similar reasons, the proposals of the NPRM are also inconsistent with the constitutional guarantee of Equal Protection. Those proposals unlawfully single out Hikvision for unequal treatment because it is Chinese, and fail even rational basis review because they are based on *irrational* logical leaps.

The Commission has also failed to identify any source of legal authority permitting it to adopt the proposed rule. As noted above, the Commission has long *disclaimed* authority to regulate peripheral devices or customer premises equipment (“CPE”). The Commission’s express authority under section 302 of the Communications Act, which authorizes the Commission’s equipment certification regime and is entitled “Devices which interfere with radio reception,” does not extend to public-interest regulation of equipment for reasons of national security.⁶ Section 302 is specifically limited to addressing potential interference from devices intentionally or unintentionally emitting radio frequencies. Yet the NPRM does not and cannot suggest that Hikvision equipment poses any threat to the United States’ (“RF”) environment or is non-compliant with the Commission’s rules. The Commission instead proposes, in an unprecedented manner, to extend its equipment authorization requirements to achieve an outcome unrelated to its RF policies. That exceeds the congressional delegation of authority under Title III.

Neither the National Defense Authorization Act (“NDAA”) nor the SNA confers any additional express authority on the Commission to regulate equipment that is not funded by the Universal Service Fund (“USF”) or purchased by government agencies. In the NDAA and the SNA, Congress made the determination to restrict *only* government funding or use of Hikvision equipment for specific places and purposes, leaving the vast majority of Hikvision’s products

⁶ 47 U.S.C. § 302a.

and end users unaffected. Even within the NDAA’s and SNA’s designated purposes, Hikvision equipment is on the Covered List only “to the extent it is used for public safety or security” and “essential to the provision of advanced communications service”⁷—yet the NPRM proposes to ban such equipment entirely. The NPRM acknowledges this mismatch, “tentatively” concluding that its proposed rules are “not specifically authorized by the Secure Networks Act itself, pursuant to which the Commission adopted the Covered List.”⁸ In fact, however, the proposals of the NPRM *contradict* Congress’s determinations in the NDAA and the SNA to limit the scope of that legislation, and they are inconsistent with the Covered List, on which they depend.

The NPRM’s proposals also exceed the Commission’s ancillary jurisdiction. The Commission may only exercise such ancillary jurisdiction where two conditions are met: “(1) the Commission’s general jurisdictional grant under Title I covers the regulated subject and (2) the regulations are reasonably ancillary to the Commission’s effective performance of its statutorily mandated responsibilities.”⁹ *Neither* requirement is satisfied here—under Title I, the Commission has no general regulatory authority over CPE that is not engaged in communications by wire or radio, and the Commission has pointed to no specific statutory provision or provisions that the proposed regulations are *reasonably* ancillary to effectuating:¹⁰

- The SNA provides no ancillary jurisdiction because the proposed rules are not reasonably ancillary to effectuating the ban on federal universal service subsidies; instead, they reach far beyond subsidized facilities to unsubsidized, private, end-user (and thus non-carrier) installations.

⁷ *National Defense Authorization Act for Fiscal Year 2019*, Pub. L. No. 115-232, §889, 113 Stat. 1636, 1919 (“2019 NDAA”); 47 USC § 1608(4).

⁸ *Covered Equipment NPRM* ¶ 65.

⁹ *American Library Ass’n v. FCC*, 406 F.3d 689, 691–92 (D.C. Cir. 2005).

¹⁰ *See Comcast Corp. v. FCC*, 600 F.3d 642, 653 (D.C. Cir. 2010).

- Section 303 and other statutory provisions outside of section 302 conferring responsibilities on the Commission relating to RF spectrum licensing and interference also provide no ancillary jurisdiction because the proposals of the NPRM have nothing to do with spectrum licensing or interference.
- The Communications Assistance for Law Enforcement Act (“CALEA”) provides no ancillary jurisdiction with respect to video surveillance equipment because CALEA applies only to network equipment, not CPE.

Finally, even if the Commission were to have authority to adopt the proposals of the NPRM, it bears emphasis that American businesses, including Hikvision’s partners and distributors as well as its end users, would bear the brunt of those onerous rules if adopted. As noted above, the market for camera security systems in the United States is highly competitive. But Hikvision has gained considerable market share in a highly competitive market by providing a technologically superior system with outstanding customer support, reliability, ease of use, and cost-effectiveness. Effectively barring Hikvision from the United States market will leave thousands of small- to medium-sized businesses without the support that they require and will ultimately impose substantial (and entirely unnecessary) costs on them as they necessarily migrate to systems that are still supported.

II. FACTUAL BACKGROUND

A. The Equipment that Hikvision Imports into the United States Does Not—and in Many Common Installations Cannot Possibly—Pose a National Security Risk to the American Public.

In the United States, Hikvision principally provides video surveillance systems for businesses.¹¹ Security cameras and video storage devices, marketed primarily to small- to medium-sized businesses by Hikvision’s retail partners, represent the vast majority of Hikvision’s sales in the United States. A typical installation by an end-user business includes

¹¹ These comments focus on the substantial Hikvision business in the United States. To this end, the comments do not address EZViz, a standalone subsidiary of Hikvision, as it is a separate company and product line with limited presence in the United States.

one or more physical cameras and a recording device, such as an NVR, that records and stores the camera's video feed. Hikvision's cameras and recorders do not require an Internet connection to operate. Like many peripheral devices, Hikvision cameras do not have a monitor/display or keyboard. The owner of a Hikvision IP camera can configure and manage it by using a web browser on a computer as long as the computer is on the same internal network as the camera. While many of Hikvision's products include Internet connection capabilities, end-user businesses can (and often do) operate Hikvision equipment on an entirely standalone basis unconnected to outside networks (including the Internet). While some Hikvision cameras also have Wi-Fi connection capabilities, these camera models also do not require connection to the Internet or an outside network in order to function.

The Hikvision products sold in the United States, if connected to telecommunications networks at all, are peripheral devices that operate outside the edge of the network, *i.e.*, on the user's side of the point at which the user's network connects to the Internet. They are accordingly *not* part of the telecommunications or Internet infrastructure. Some devices may be configured to communicate with one another via telecommunications networks, such as when using a VPN over an enterprise WAN, but the cameras and NVRs are all CPE installed at the end users' locations. Hikvision cameras and NVRs are not and cannot be used by telecommunications carriers or Internet Service Providers ("ISPs") to route or manage telecommunications or Internet traffic.

Hikvision cameras can be deployed by end users in several ways: a standalone, physically isolated deployment; a standalone, logically separated deployment; or, if the end user chooses, with direct Internet connectivity. Each of these deployments has its own defenses against

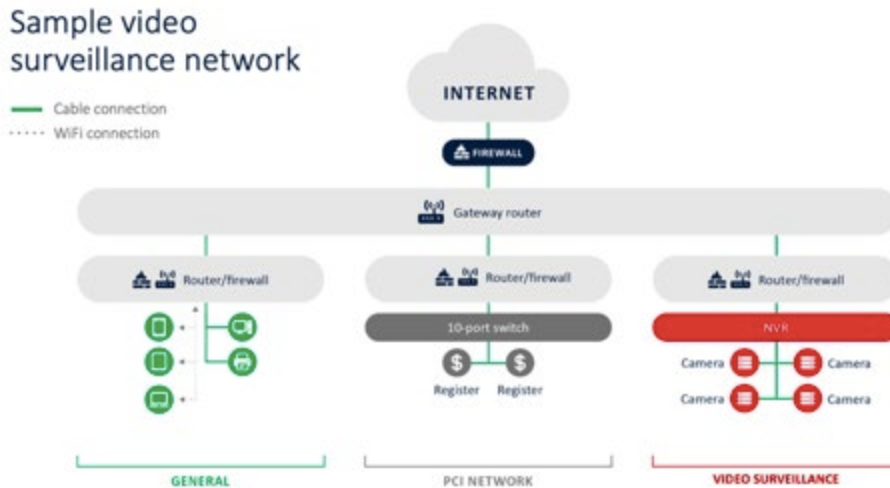
cyberattacks by any party, including a hypothetical attack by Hikvision itself—although there has, of course, never been any evidence of any such efforts by the company.

Standalone, physically isolated deployment. In a standalone deployment, Hikvision equipment can operate over a private, isolated network without being connected to—and therefore remaining physically separate from—the Internet. For instance, a convenience store might install multiple cameras inside the store, in the loading dock, and on the exterior that all connect to a single NVR that is also on the premises. These cameras can all be connected to a single NVR, which records the video feed for later playback if needed. The cameras and NVR are all connected to ports on a single switch, which could be connected to a monitor screen at the cash register; an employee standing at the register would then be able to view the feed from the cameras in real time or play back the recorded video feed from the NVR at a later time. The connections between the devices might be made by coaxial cable, ethernet cable, or Wi-Fi connections. But regardless of how the devices are connected to one another, in this common “standalone” deployment, none of the Hikvision equipment would be connected to the Internet or an Internet-connected device at all. They remain physically and logically isolated from the Internet.

A business could also install one or more security cameras and create a wired connection directly between the camera and a computer. In this alternative deployment, the equipment is not running on an internal network at all (the camera and computer would make up an isolated network of just those two devices). Instead, the camera’s video feed connects directly through cables to the computer and can be viewed in real-time. Accordingly, in this deployment as well, none of the equipment is connected to the Internet or to Internet-connected devices.

These types of never-connected-to-the-Internet deployments are sometimes referred to as “air gap” deployments because there is a gap of air between the deployed equipment and the Internet. As a result, there is no threat of an inbound cybersecurity attack because there is no connection to an outside network and therefore no point of entry from which a third party could attempt to connect to the Hikvision equipment. Similarly, there is no threat of “malware” (malicious software) in the devices creating an outbound export of data from the video surveillance system because the system is not connected to any outside network to which the data could be exported—the data has nowhere to go. Because the Hikvision equipment is physically isolated from the Internet, no third party can access the cameras or recorder remotely. This is true regardless of whether the Hikvision equipment is interconnected by ethernet cable or Wi-Fi—again, the devices do not require any connection to the Internet in order to operate on a closed network.

Standalone, logically separated deployment. Some businesses deploy Hikvision equipment over an internal network that has Internet access, but isolate the Hikvision equipment on a logically separated network from other devices on the internal network. In this scenario, the internal network is protected from inbound Internet attacks by deploying a firewall at the network’s edge. Behind that firewall are network segments that protect one internal network from the other by deploying internal firewalls. As a best practice, Hikvision highly recommends that end users logically separate their video surveillance devices from other internal devices and ensure that all internal devices are protected from Internet-sourced attacks by deploying a firewall. This solution allows the end-user network’s IT administrator to decide whether to give all devices on both internal networks access to the Internet, or just those on some networks, with inbound access to the devices blocked by the firewall.



A business may choose to logically separate its Hikvision equipment from the rest of the internal network by using multiple router/firewalls or a managed switch to create separate Virtual Local Area Networks (“VLANs”) and assigning ports on the switch to only one of the networks. For instance, an end-user retail clothing store might have four cameras in different parts of the store, all connected to a single NVR. The clothing store might also have two registers for processing retail transactions. The store may also have a few computers, printers, and mobile devices for conducting back-office business like inventory, payroll and accounting. Cybersecurity best practice is to segment each of these networks so the devices from one network are unable to communicate with devices from the other network. However, depending on the choices made by the end user’s IT administrator, they may all have Internet access through the gateway router/firewall, or only some.

This separation of networks means that if someone falls for a phishing email on a computer, that malware-infected computer would not be able to gain access to the cash registers or the video surveillance equipment since they are on separate networks. Significantly, the owner of the network firewalls has the ability to block all inbound and outbound traffic to each

of the separate, internal networks if they desire. In this scenario, no data can get in and none can flow out of that blocked network as it has been logically isolated.

Internet-connected deployment. There are essentially two reasons to grant Internet access to a Hikvision device. The first reason is to easily download and update firmware that may add new features or bug fixes. This can be accomplished in an isolated deployment but it takes a few extra steps. The second reason is so the owner of the Hikvision devices is able to remotely access their Hikvision devices. This second reason is likely the most popular reason to give Hikvision devices access to the Internet.

There are three basic solutions for remotely monitoring and managing a video surveillance network.

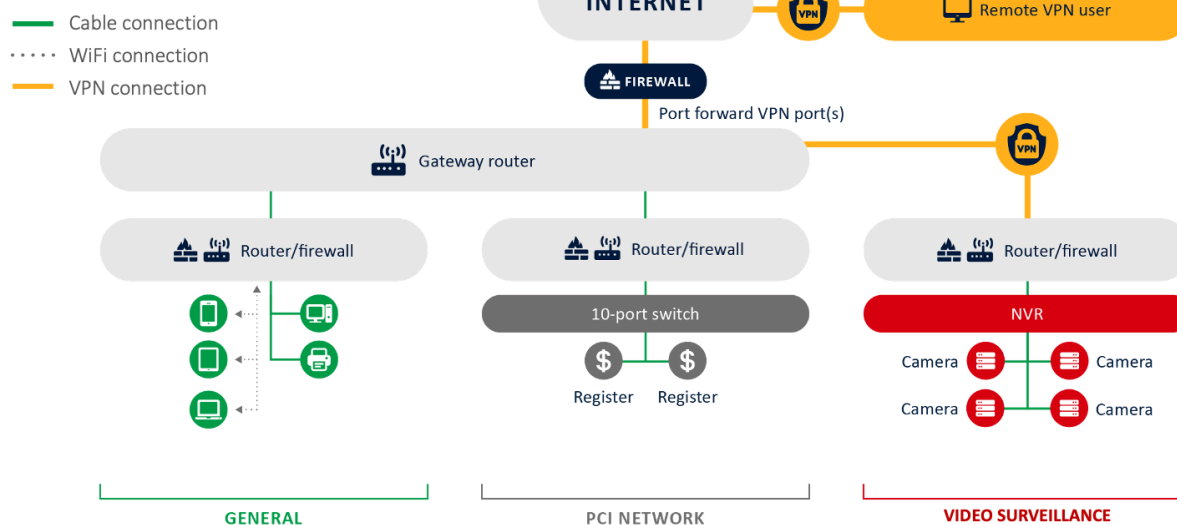
1. *Use a VPN.* The VPN provides encrypted access to the internal video surveillance network so that only the people who have the appropriate credentials can gain access to the cameras and NVRs. This is the most secure and recommended solution.
2. *Use a cloud-based access control tool.* There are many cloud-based solutions available to Hikvision users, including Hikvision's own Hik-Connect solution. This solution provides a direct, end-to-end encrypted connection between the smartphone of a camera owner and his or her camera(s). This is a secure solution, but not as secure as using the VPN.
3. *Port-forward your Hikvision device only when absolutely necessary.* This solution will make the camera or NVR directly accessible from anyone on the Internet. The only thing stopping someone from gaining access to the

device is the strength of the user's password. While this is an easy and effective solution, port forwarding is very risky. Hikvision cautions its end users against port forwarding, and advises that "port forwarding should only be configured when absolutely necessary."¹² Where end users affirmatively choose to configure port forwarding for devices that need to be accessed via the Internet, Hikvision supports the following cybersecurity best practices: (1) "minimize the number of ports exposed to the Internet," (2) "avoid using generic ports and reconfigure them as custom ports," (3) "enable IP filtering," (4) "set a strong password," and (5) "upgrade to the latest device firmware released by Hikvision, in a timely manner."¹³

¹² Hikvision, *Network Security Hardening Guide*, at 23, https://us.hikvision.com/sites/default/files/hardening_guide.pdf (v 1.2 2017).

¹³ *About "Port Forwarding"*, Hikvision (2018), [about-port-forwarding-hikvision.pdf](https://s3.amazonaws.com/ipvm-uploads/about-port-forwarding-hikvision.pdf) (ipvm-uploads.s3.amazonaws.com).

VPN to video surveillance network



As just explained, Hikvision cameras—including those with Wi-Fi—do not require Internet connectivity to function, and end users can and do choose to operate their devices while remaining physically or logically isolated from the Internet. Because Hikvision does not sell directly to end users, it has limited information about how specific devices are installed,¹⁴ but only a very small percentage of Hikvision devices appear to be directly connected to the Internet.

In this kind of situation, an end user can implement Hikvision’s other cybersecurity best practices to protect Hikvision equipment. (All of these best practices can also be implemented, if an end user chooses, in a standalone, logically separated deployment.) End users can also protect their Hikvision equipment by implementing Hikvision’s recommendations to use a strong password, to enable password lock-out features for invalid device login attempts, and to enable the illegal login lock feature, limiting the number of user login attempts from a particular IP address, thereby defending against “brute force” password attacks.

¹⁴ See *infra* at Part II.C (discussing the fact that Hikvision does not collect end-user data).

As noted above, in order to protect against an outbound transmission of data, a business can set up firewall rules to block all outbound traffic from Hikvision devices. If there is a need to have a Hikvision device communicate with a system on the Internet, the firewall rule can be created to allow only the approved outbound traffic. Even if the closed network is not isolated, Hikvision's rigorous pre-deployment testing of its software, regular monitoring of deployed software, and availability to deploy software patches thwart any attempt by malware to create an outbound export of data.

B. Hikvision Is a Globally Respected Video Surveillance Company.

Hikvision is a world leader in the field of comprehensive security. Hikvision has operated in the United States since 2006. In the past ten years, Hikvision security systems have been sold through approximately 50,000 independent dealers in the United States. As of 2020, Hikvision was ranked third in the highly competitive video surveillance market in the United States, with a market share of 14.3 percent.¹⁵

Hikvision was established in 2001 and has been publicly traded on the Small and Medium Enterprise Board ("SME Board") in China's Shenzhen Stock Exchange since May 2010. Hikvision has a diverse set of private and public shareholders. Hikvision's founder, Hong Kong resident Kung Hung Ka (also written Gong Hongjia), is the company's second largest shareholder. Its largest shareholder is China Electronics Technology Group Corporation ("CETC"), a Chinese state-owned enterprise, that is not involved in the day-to-day operations of the company. Notably, in the United States and Canada, Hikvision is operated as separate subsidiaries, employing more than 200 professionals, and headquartered in City of Industry, California and Ontario, Canada respectively.

¹⁵ Mordor Report at 164.

C. Hikvision Products Are Not Sold Directly to American Consumers.

Hikvision does not sell its products directly to consumers in the United States. Nor does it sell products directly to the U.S. government. Any such sales would be undertaken by Hikvision dealers. For that reason, Hikvision's sales process does not produce (and the company does not maintain) systematic information about the identities of end users. Hikvision also does not collect end-user data through its warranty registration or returns process—instead, that process is handled by Hikvision's dealers.¹⁶ Because Hikvision simply does not collect or maintain end-user data, the threat of any targeted cyberattack on Hikvision end users by anyone accessing company data—whether from inside or outside of the company—is virtually non-existent. Moreover, with regard to unsubstantiated concerns about Hikvision providing data to the Chinese government, its approach to sales and service means that it lacks any significant amount of end-user data to provide.

D. Only a Limited Number of Hikvision Product Models Are Sold in the United States, and Those Products Undergo Extensive Software Testing and Mostly Do Not Require Network Connectivity.

The Hikvision products available in the United States are limited. Those products primarily include cameras, NVRs, switches, and software.¹⁷ Hikvision offers select camera

¹⁶ See *RMA Policy*, Hikvision, <https://us.hikvision.com/en/support-resources/warranty-rma/rma-policy> (last visited Sept. 18, 2021); *RMA Request Form*, Hikvision, https://us.hikvision.com/sites/default/files/hikvision_rma_request_form.pdf (last visited Sept. 18, 2021).

¹⁷ Cameras and NVRs make up the majority of Hikvision products sold in the United States. Several other product lines make up the remaining small fraction of Hikvision's U.S. sales: software, access control devices, video intercom devices, security radar, encoder/decoder, digital signage box, ethernet switches, monitor, and accessories. For example, Hikvision's access control devices include an access controller, magnetic door lock, card reader, fingerprint reader, identity authentication, terminal, and walkthrough metal detector. Hikvision's other products available in the United States function in a manner analogous to

models for sale in the United States, from product lines including Network, Network PTZ, TurboHD, Thermal, Value Express Indoor Dome and Outdoor Dome, Turret, Box, Cube, and Bullet cameras. These cameras range from very basic models to cutting edge designs incorporating, for example, sensing technologies that recognize objects and faces.

As noted above, Hikvision's security cameras most commonly operate with an NVR or equivalent recording device. An NVR generally also permits end users to consolidate video feeds from multiple cameras and to output them for display, such as to a monitor. The NVR also records and stores video feed for playback later.

As also noted above, no Hikvision equipment sold in the United States is essential communications equipment, and no Hikvision equipment is used in fixed or mobile broadband networks. Only about five percent of Hikvision devices sold in the United States contain radio transmitters, and thus only a small number are certified pursuant to the Commission's equipment certification process. The remainder—approximately ninety-five percent—are manufactured, imported, and operated in the United States pursuant to the Commission's Supplier's Declaration of Conformity ("SDoC") process, which is used for equipment that does not contain radio transmitters and thus are not intentional radiators.

1. Hik-Connect and HikCentral

Hikvision's only current offering in the United States that *requires* Internet connection is Hik-Connect, an optional mobile platform that permits users who choose to enable the feature to view information from their video surveillance systems on Android and Apple smartphones and tablets using the Hik-Connect mobile app, and on Windows and Mac computers using the

the cameras and NVRs described herein, with the end user controlling the operation of the device.

iVMS4200 client software. Hik-Connect represents a very small percentage of Hikvision's business in the United States. iPhone users can download the Hik-Connect app from the Apple store, and Android users can download it from Hikvision's website.¹⁸ Hik-Connect is disabled by default, and Hikvision advises that access to Hik-Connect should be enabled only if needed. When an end user enables Hik-Connect on their camera, they will create a free account on the Hik-Connect server. Then their camera will reach beyond the end user's firewall to send its public IP address information to the Hik-Connect server. This happens on a regular basis since many ISPs frequently change IP addresses of homes and small businesses. After initially setting up the camera to use Hik-Connect, the end user would install the Hik-Connect app and log into the account they created when setting up Hik-Connect on the camera. When the end user wants to remotely view their camera, they log into the Hik-Connect app from their mobile device and they will see a list of the devices that they have registered with Hik-Connect. If they tap on one, the Hik-Connect server will send the IP address of the camera to the user's smartphone and the phone and camera will initiate a direct, end-to-end encrypted connection. The Hik-Connect server thus acts almost like a phone book for the camera and the app. No audio or video data is being stored or accessed by the Hik-Connect server.¹⁹

Hikvision also offers an optional comprehensive management system called HikCentral. HikCentral is a modular software platform consisting of multiple software clients that work

¹⁸ Hikvision, *Hik-Connect Remote Access Platform and Mobile App*, at 1 (2020), https://us.hikvision.com/sites/default/files/data_sheet/hik-connect_sw_101620na.pdf.

¹⁹ In North America, Hikvision deploys Hik-Connect utilizing an Amazon Web Services server located in the United States. In addition, other servers, also located in the United States but owned by Tencent Cloud and Ucloud, are used to provide Hik-Connect Streaming Media Service, which allows users to view live video. All of the servers transmit encrypted data; again, no audio or video data is stored in or visible to any of the servers.

together to permit end users who opt to utilize HikCentral to manage multiple Hikvision devices—such as access controls and facial terminals—from a single point of control. An enterprise using HikCentral can integrate and monitor all its video surveillance devices together with functionality such as alarms and logs. HikCentral is not necessary to the operation of any Hikvision cameras, NVRs, or switches.

For example, Control Client—installed at a client location—is used for daily monitoring in real time. It includes functionalities such as live view and playback, and enables end users to tag relevant video clips so that they can be searched, stored, and viewed by trusted parties. It allows multiple systems to be brought together and managed through a single graphical user interface, thereby reducing overall operational costs compared to control.

HikCentral also offers a Web Client, permitting end users to access management of the system from anywhere via a web browser. The Web Client allows users to add devices, configure camera recording schedules, assign user rights, access camera live views and playback, and so on. HikCentral also offers a Mobile Client, allowing the management capabilities of the software to be accessed via mobile devices.

HikCentral software gives end users the ability to centralize management of regional, national, or global security systems, and that kind of integration of course requires an Internet connection. But, as for Hik-Connect, the end user retains control over their data—it is not visible to or stored by Hikvision.

2. Software

Hikvision’s software, including both software for its devices and enterprise software, undergoes extensive testing prior to implementation and release to the public. This testing includes searching for known vulnerabilities, such as performing security code scanning and

using vulnerability scanners. Hikvision also tests for unknown vulnerabilities by using a “fuzzing” tool. That tool randomly directs data to the software being tested in an effort to search for vulnerabilities in the software. Any vulnerabilities exposed through this process are then patched by the software developer.

After Hikvision software is released to the public, end users can and do report vulnerabilities to the Hikvision Security Response Center. Hikvision then creates a patch to address the reported vulnerability, which is made available to end users. Hikvision is responsive to vulnerabilities and is quick to push out updates to its end users. For example, in March 2017 a security researcher found and reported a vulnerability—six days later, Hikvision released a firmware patch, notified its partners through a special bulletin, and notified the public with a notice on its website.²⁰ In response to questions in a January 2018 House Small Business Committee hearing about Hikvision equipment vulnerabilities, Richard Driggers, Deputy Assistant Secretary for the Department of Homeland Security (“DHS”) Office of Cybersecurity and Communications, stated that once a vulnerability was discovered, “we worked with [Hikvision]” and Hikvision “put out a software update that mitigated the impacts of this

²⁰ In September 2021, Hikvision disclosed a “zero click remote code execution” vulnerability and released patches to fix the vulnerability on the same day. Hikvision, *Security Notification- Command Injection Vulnerability in Some Hikvision Products* (Sept. 18, 2021), <https://us.hikvision.com/en/support-resources/documentation/special-notice/security-notification-command-injection>. Because the vulnerability is exploitable by an attacker who has accessed the device network, it affects devices which end users may choose to connect to the Internet. As discussed above in Part II.A, however, Hikvision strongly advises against port forwarding because many more secure methods of deployment are available. Notably, refining defenses against zero-click attacks remains a challenge for a wide variety of hardware and software companies, which are similarly situated to Hikvision in this regard.

particular exploitation . . . [a] standard practice that we do at the Department of Homeland Security across many different companies’ devices and software.”²¹

The Hikvision Network and Information Security Lab utilizes the world’s leading known-vulnerability scanning tools and unknown-vulnerability discovery tools to verify and ensure that Hikvision products meet the industry cybersecurity standards and regulations.

Hikvision also hires third parties, such as U.S.-based cybersecurity company Rapid7, to test for and identify vulnerabilities so that Hikvision can address them during the testing process. In 2015 and 2017, Hikvision conducted a penetration test with Rapid7 on two Hikvision cameras and two NVRs. That penetration test found no critical vulnerabilities. In 2018, Hikvision entered into a partnership with SGS—now SGS Brightsight—one of the leading global inspection and certification companies, to serve as the laboratory of choice for Hikvision’s range of security products.²² As a result of that partnership, SGS Brightsight certified Hikvision’s network camera series, V5.5.60, using the Common Criteria (“CC”) version 3.1 revision 5. CC provides assurance that the process of specification, implementation, and evaluation of a computer security product has been conducted in a rigorous, standard, and repeatable manner at a level that is commensurate with the target environment for use.

In 2019, U.S.-based certification company UL was asked to study three Hikvision camera models and perform a source code review of their software components. UL’s report identified no issues as to chain-of-trust, sensitive data, device hardening, configuration management, and

²¹ House Small Business Committee, *Small Business Information Sharing: Combating Foreign Cyber Threats*, YouTube (Jan. 30, 2018), <https://www.youtube.com/watch?v=vWiBWkpvIAA&t=1575s>.

²² See generally *Who we are*, SGS Brightsight, <https://www.brightsight.com/about> (last visited Sept. 18, 2021).

security incident response plan; and it identified only low risk as to secure software update, authentication of services, network protocols and interfaces, and debug interface.

E. The Interoperability of Hikvision Equipment Is a Defense Against Potential Cyberattacks.

Hikvision cameras support the Open Network Video Interface Forum (“ONVIF”) standard, which is a manufacturer interoperability standard. That interoperability capability means that Hikvision’s cameras will operate with an NVR made by Hikvision or with an NVR made by one of Hikvision’s competitors. Similarly, Hikvision cameras will operate with an off-the-shelf server or with a computer with appropriate Hikvision software or third-party software, such as Milestone Systems or AxxonSoft software.

The ability to use Hikvision equipment with non-Hikvision hardware and non-Hikvision software creates additional cybersecurity protection through “defense in depth.” Because Hikvision equipment can be—and is—used with non-Hikvision equipment, any potential inbound threat would need to penetrate not only Hikvision’s considerable cybersecurity defenses, but also the cybersecurity defenses of the companies that manufactured the non-Hikvision equipment. This mix-and-match functionality builds on the protections already offered by Hikvision’s deployment options.

F. Cybersecurity Is of Paramount Importance to Hikvision.

Hikvision is constantly working to optimize its cybersecurity in development, manufacturing, delivery, and servicing of its video surveillance products. As part of its cybersecurity efforts, Hikvision complies with all applicable national and regional cybersecurity regulations and follows best industry practices. It has established a sustainable and reliable cybersecurity assurance system that encompasses the company’s policies, organizational and operational procedures, and technology and regulations.

Hikvision also engages with third-party cybersecurity certifiers to test its products for cybersecurity certifications and recognitions. For some certifications, the testing process takes several months and requires multiple rounds of testing. Hikvision has received numerous cybersecurity certifications and recognitions. For instance, Hikvision has obtained various certifications developed by the International Organization for Standardization (“ISO”) and the International Electrotechnical Commission (“IEC”) and conducted by external certification bodies.²³ Hikvision has received the international information security standard ISO 27001:2013, which “specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organization.”²⁴ It has also received ISO 28000:2007, which “specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain,”²⁵ and ISO 9001:2008, which:

specifies requirements for a quality management system where an organization needs to demonstrate its ability to consistently provide product that meets customer and applicable statutory and regulatory requirements, and aims to enhance customer satisfaction through the effective application of the system, including processes for continual improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements.²⁶

Additionally, Hikvision has received the information technology service management system standard ISO/IEC 20000-1:2011, which “specifies requirements for an organization to establish, implement, maintain and continually improve a service management system,”

²³ *Certification*, ISO, <https://www.iso.org/certification.html> (last visited Sept. 18, 2021).

²⁴ *ISO/IEC 27001:2013*, ISO, <https://www.iso.org/standard/54534.html> (last visited Sept. 18, 2021).

²⁵ *ISO 28000:2007*, ISO, <https://www.iso.org/standard/44641.html> (last visited Sept. 18, 2021).

²⁶ *ISO 9001:2008*, ISO, <https://www.iso.org/standard/46486.html> (last visited Sept. 18, 2021).

including “the planning, design, transition, delivery and improvement of services to meet the service requirements and deliver value.”²⁷

Hikvision has also achieved Capability Maturity Model Integration (“CMMI”) Level 5, a process improvement model that is required by many Department of Defense and U.S. government software development contracts.²⁸ CMMI “helps organizations streamline process improvement and encourage productive, efficient behaviors that decrease risks in software, product, and service development.”²⁹ It breaks down organizational maturity into five levels, and once an organization achieves Levels 4 and 5, they are considered “high maturity,” where they are “continuously evolving, adapting and growing to meet the needs of stakeholders and customers.”³⁰

Additionally, Hikvision has received a Level 1 Federal Information Processing Standard (“FIPS”) 140-2 certification, issued by the Computer Division of the National Institute of Standards and Technology (“NIST”).³¹ FIPS 140-2 is an information technology security accreditation standard for validating that a cryptographic module—“the set of hardware, software, and/or firmware that implements security functions”—meets well-defined security requirements, “cover[ing] cryptographic module interfaces; software and firmware security; operating environment, physical security; security parameter management; self-tests; mitigation

²⁷ *ISO/IEC 20000-1:2018*, ISO, <https://www.iso.org/standard/70636.html> (last visited Sept. 18, 2021).

²⁸ Sarah K. White, *What Is CMMI? A Model for Optimizing Development Processes*, CIO (June 1, 2021), <https://www.cio.com/article/2437864/process-improvement-capability-maturity-model-integration-cmmi-definition-and-solutions.html>.

²⁹ *Id.*

³⁰ *Id.*

³¹ *FIPS 140-2: Security Requirements for Cryptographic Modules*, NIST, <https://csrc.nist.gov/publications/detail/fips/140/2/final> (last visited Sept. 18, 2021).

of attacks; and roles, services, and authentication.”³² Notably, federal agencies “that operate cryptographic modules or have contracts to have the modules operated for them must have the modules they use pass tests for these requirements.”³³ Level 1 “covers the basic security features in a cryptographic module.”³⁴ Hikvision was one of the first video surveillance companies to receive this certification, widely recognized as the de facto standard for cryptographic modules, for both its camera and NVR products.

Hikvision has also obtained for its network camera series CC certification with assurance type EAL2 augmented with ALC_FLR.2 (EAL2+),³⁵ an international standard for computer security certification developed by the governments of the United States, Canada, France, Germany, the Netherlands, and the United Kingdom, building upon earlier standards.³⁶ CC provides “assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous, standard and repeatable manner at a level that corresponds with its target use environment.”³⁷ To achieve this certification, the Hikvision network camera series was evaluated at the Norwegian evaluation facility using Common Methodology for IT Security Evaluation.

³² Connor Craven, *What Does It Mean To Be FIPS Compliant?*, SDxCentral (Feb. 19, 2020), <https://www.sdxcentral.com/security/definitions/what-does-mean-fips-compliant/>.

³³ *Id.*

³⁴ *Id.*

³⁵ Hikvision Dig. Tech. Co., *Hikvision Achieves Common Criteria Certification*, CISION PR NEWswire (Oct. 9, 2018), <https://www.prnewswire.com/il/news-releases/hikvision-achieves-common-criteria-certification-696212031.html>.

³⁶ Nancy Mead, *The Common Criteria*, Cybersecurity & Infrastructure Security Agency, <https://us-cert.cisa.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria> (last revised July 5, 2013).

³⁷ Katie Moss Jefcoat, *What Is Common Criteria Certification, and Why Is It Important?*, BLANCCO (Dec. 8, 2017), <https://www.blancco.com/resources/blog-what-is-common-criteria-certification-why-is-it-important/>.

In light of Hikvision’s many cybersecurity efforts, it is not surprising that its end users in the United States regard Hikvision products highly.³⁸ Indeed, a U.S. distributor of its products wrote, “Hikvision System is a superior system in the industry. The excellent support, reliability, the ease of use, the cost, the functionality as well as the level of security of the system are unmatched.”³⁹

G. Hikvision Empowers End Users to Implement Cybersecurity Measures to Protect Against Inbound Attacks and Outbound Transmission.

Although Hikvision devotes substantial effort to ensure the greatest device protection for its products, it is also essential for end users to understand how to install and use Hikvision’s cameras and NVRs as securely as possible. To this end, Hikvision invests in providing its end users and distributors in-depth information about cybersecurity measures for its equipment. The Hikvision website includes interactive webinars “revolving around Hikvision’s systematic solutions that solve real-world problems”⁴⁰ and guidance on best security practices in its Cybersecurity Center.⁴¹ Hikvision’s best practices include ten safeguards against a potential cyberattack, including regularly updating software and firmware, creating a secure password and password lock-out features for invalid device login attempts, and using a firewall appliance between IT assets and the Internet.⁴² Hikvision makes available to the public cybersecurity white papers on issues such as the inadvisability of port forwarding from a cybersecurity

³⁸ See, e.g., Letter from Doug Haynes, Gen Net, Inc., to Marlene Dortch, Secretary, FCC, ET Docket Nos. 21-232, 21-233 (filed Aug. 24, 2021).

³⁹ *Id.*

⁴⁰ *Webinars*, Hikvision, <https://www.hikvision.com/en/webinars/> (last visited Sept. 18, 2021).

⁴¹ *Best Practices*, Hikvision, <https://us.hikvision.com/en/support-resources/cybersecurity-center/best-practices> (last visited Sept. 18, 2021).

⁴² *Id.*

perspective, product security, network camera security, NVR security, and the Zero Trust concept of addressing cybersecurity concerns.

In addition to the information provided on its website, Hikvision both communicates and encourages cybersecurity best practices by sending periodic emails to its partners and distributors. Hikvision also distributes a cybersecurity newsletter and updates a cybersecurity blog. Hikvision highly recommends that end users regularly check for and upgrade to the latest available firmware to ensure any security updates are installed. When Hikvision software or firmware updates are made available, Hikvision sends out an alert that the update is available and directs the end user to download it from Hikvision’s website and install it, which protects the end user from having to unnecessarily connect their device to the Internet solely for software-update purposes.⁴³

Hikvision makes available education modules—which are thirty-minute videos on best practices—to the public. Further, Hikvision requires that its salespeople, engineers, and employees take courses in cybersecurity, and creates and distributes short educational guides on cybersecurity topics—including product security—for its salespeople, engineers, and employees.

III. THE COMMISSION LACKS ANY EXPRESS OR ANCILLARY AUTHORITY TO ADOPT THE PROPOSALS OF THE NPRM.

A. Title III Provides the Commission Authority to Manage the RF Spectrum and Potential Interference, but No General Authority to Regulate on Public Interest or National Security Grounds.

In the NPRM, the Commission announces its intent to “leverage” its authority over equipment authorization “to help keep untrusted vendors and equipment out of U.S. networks.”⁴⁴

⁴³ Some newer Hikvision products have an automatic download feature, which the end user can choose to enable if the device has access to the Internet.

⁴⁴ *Covered Equipment NPRM* ¶ 4.

But Congress has not authorized the Commission to police the nation’s equipment markets based on the Commission’s level of “trust” in different manufacturers. Title III provides the Commission authority to regulate the RF spectrum and the potential for interference within it. But the NPRM contains no suggestion that Hikvision devices pose any threat to the United States’ RF environment or that those devices are in any way non-compliant with the Commission’s RF regulation. In the absence of any RF issue, the Commission cannot transform its Title III jurisdiction over spectrum into general authority to regulate in the “public interest” contrary to Congress’s direction.

But that is precisely what the NPRM proposes to do—to use the Commission’s authority over equipment authorization to address hypothetical national security concerns in connection with purportedly “untrusted vendors.” The NPRM cites sections 302 and 303 as potentially allowing it “to deny equipment authorization to equipment deemed to pose an unacceptable security risk.”⁴⁵ But those provisions of Title III do no such thing. While Title III does give the Commission “expansive powers” to encourage “*more effective use of radio in the public interest*,” it does not “confer an unlimited power.”⁴⁶ Indeed, the courts have made clear that “the Commission may not rely on Title III’s public-interest provisions without mooring its action to a distinct grant of authority in that Title.”⁴⁷ The Commission does not and cannot do that here.

Section 302—entitled “Devices which interfere with radio reception”—permits the Commission to “make reasonable regulations . . . governing the *interference potential* of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction,

⁴⁵ *Id.* ¶¶ 66–67; 47 U.S.C. §§ 302a, 303.

⁴⁶ *Nat’l Broad. Co. v. United States*, 319 U.S. 190, 216–17, 219 (1943) (emphasis added).

⁴⁷ *Cellco P’ship v. FCC*, 700 F.3d 534, 542 (D.C. Cir. 2012).

or other means in sufficient degree to cause harmful interference to radio communications.”⁴⁸

Section 302 also authorizes the Commission to “establish[] minimum performance standards for home electronic equipment and systems to reduce their susceptibility *to interference* from radio frequency energy.”⁴⁹ The provision further specifies that the Commission shall apply “[s]uch regulations . . . to the manufacture, import, sale, offer for sale, or shipment of such devices and home electronic equipment and systems, and to the use of such devices.”⁵⁰ Each provision of section 302 thus limits the Commission’s regulatory authority over importation and use of devices to adopting measures to address *RF emissions*.⁵¹

The Commission nonetheless suggests that “the ‘public interest’ phrase” in section 302 might allow it to decline to “approve devices capable of . . . caus[ing] harmful interference” if they “pose an unacceptable risk to the national security of the United States.”⁵² But that phrase does not expand the Commission’s authority. The language and structure of section 302 are clear—that section does not say that the Commission may make rules of unlimited scope governing equipment so long as it finds a rule would be “consistent with the public interest,

⁴⁸ 47 U.S.C. § 302a(a) (emphasis added).

⁴⁹ *Id.* (emphasis added).

⁵⁰ *Id.* (emphasis added).

⁵¹ Section 302 also contains additional express limitations on its application—it does not apply, for example, to “carriers transporting such devices or home electronic equipment and systems without trading in them, to devices or home electronic equipment and systems manufactured solely for export, to the manufacture, assembly, or installation of devices or home electronic equipment and systems for its own use by a public utility engaged in providing electric service, or to devices or home electronic equipment and systems for use by the Government of the United States or any agency thereof.” 47 U.S.C § 302a(c). Such exclusions are inconsistent with the Commission’s invocation of the provisions of section 302 to adopt a near-total ban, since they would plainly be unnecessary in the presence of a complete ban.

⁵² *Covered Equipment NPRM* ¶ 67.

convenience, and necessity.”⁵³ To the contrary, in section 302(a)—the subsection that authorizes the Commission to create equipment rules—the phrase “consistent with the public interest, convenience and necessity” directly modifies the Commission’s authority to “make reasonable regulations . . . governing the interference potential of devices.”⁵⁴ It thus does not expand the Commission’s authority *beyond* RF interference; it imposes a *limitation* on the Commission’s authority over RF interference. Accordingly, rules that do not “govern[] . . . interference potential” exceed the Commission’s power under section 302(a)—whether or not the Commission thinks such rules would otherwise serve the public interest.

The NPRM’s tentative conclusion that “it would appear to be in the public interest not to approve devices capable of emitting RF energy in sufficient degree to cause harmful interference to radio communications if such equipment has been deemed, pursuant to law, to pose an unacceptable risk to the national security of the United State or the security and safety of United States persons” is nonsensical. Under section 302, the Commission has the authority not to authorize devices that are capable of emitting RF energy sufficient to cause harmful interference, irrespective of any national security concerns. But it turns section 302 on its head to suggest that equipment that meets the Commission’s applicable RF emissions standards can nonetheless be banned because of national security concerns. The national security concerns are unrelated to RF interference under the Commission’s own, promulgated standards.

The NPRM suggests that the Commission has previously “relie[d] on the equipment authorization process to implement other statutory duties,” but the NPRM’s examples confirm

⁵³ See 47 U.S.C. § 302a(a).

⁵⁴ *Id.*

the limits of the Commission’s power.⁵⁵ Most of the examples—“the duty to promote efficient use of the radio spectrum, [the] duties under the National Environmental Policy Act [(“NEPA”)] to regulate human RF exposure, [the Commission’s] duty to ensure that mobile handsets are compatible with hearing aids”—relate directly to RF emissions, and thus do not suggest an unmoored power to make rules in the “public interest.”⁵⁶ Moreover, both NEPA and the Hearing Aid Compatibility Act of 1988 were separately enacted statutes explicitly conferring responsibilities on the Commission.⁵⁷ The final example—“the duty to deny federal benefits” to people convicted of certain federal drug crimes—is mandated by a specific statutory directive enacted by Congress, which does not exist here.

Section 302(b) likewise does not expand the scope of the Commission’s authority to regulate devices beyond RF emissions. That section provides that “no person shall manufacture, import, sell, offer for sale, or ship devices or home electronic equipment and systems, or use devices, *which fail to comply with regulations promulgated pursuant to this section.*”⁵⁸ On its face, then, section 302(b) is limited to “regulations promulgated pursuant to this section”—which necessarily cannot be more expansive than 302(a). It does not authorize rules that exceed the scope of 302(a).

Section 303 grants the Commission express authority to regulate radio broadcasting and related RF interference. Section 303(a)–(d) allow the Commission to classify radio stations and

⁵⁵ *Id.* ¶ 65.

⁵⁶ *Id.*

⁵⁷ See further discussion of the Commission’s limited authority under these statutes *infra* at Part III.D.

⁵⁸ 47 U.S.C. § 302a(b) (emphasis added).

assign them specific bands and operation powers. Section 303(e), cited by the NPRM,⁵⁹ must be read in that context—it allows the Commission to “[r]egulate the kind of apparatus to be used with respect to its external effects and the purity and sharpness of the emissions from each station and from the apparatus therein.”⁶⁰ Like 302(a), then, section 303(e) focuses on the devices’ “effects” *in the RF spectrum*. Section 303(e) accordingly does not provide the Commission authority to prevent the marketing and sale of equipment unrelated to its effects in the RF spectrum.⁶¹ Contrary to the suggestion in the NPRM, whether it is “used” or “to be used” does not expand the scope beyond RF emissions.⁶² Section 303(f) further authorizes “such regulations not inconsistent with law as it may deem necessary to prevent interference between stations and to carry out the provisions of this chapter,”⁶³ while section 303(g)—also cited by the NPRM⁶⁴—permits the Commission to “[s]tudy new uses for radio, provide for experimental uses of frequencies, and generally encourage the larger and more effective use of radio in the public interest.”⁶⁵ Those provisions thus also do not provide any authorization to exceed the scope of 302’s focus on the RF spectrum and interference. But the NPRM’s proposed broad ban on Hikvision equipment authorizations has nothing to do with uses of the RF spectrum

⁵⁹ *Covered Equipment NPRM* ¶ 66.

⁶⁰ 47 U.S.C. § 303(e).

⁶¹ *See Covered Equipment NPRM* ¶ 66 (inquiring whether “Congress’s inclusion of the phrase ‘to be used,’ rather than ‘used,’ give[s] the Commission authority to prevent the marketing and sale of equipment in addition to preventing licensees and others from using such equipment?”).

⁶² *Id.*

⁶³ 47 U.S.C. § 303(f).

⁶⁴ *Covered Equipment NPRM* ¶ 65.

⁶⁵ *Id.* § 303(g).

or with RF interference and section 303, like section 302, thus provides no express authority for it.

B. The Proposals of the NPRM are Inconsistent with Section 889 of the NDAA and the Secure Networks Act.

In the *Supply Chain Second Report and Order*,⁶⁶ the Commission undertook implementation of section 889 of the NDAA⁶⁷—prohibiting the use or procurement of certain telecommunications equipment by executive agencies and government contractors—and the SNA’s requirement to publish a “Covered List” of equipment posing an unacceptable risk to national security.⁶⁸ In addition to its misplaced reliance on Title III, the NPRM attempts to bootstrap section 889, the SNA, and the resulting Covered List into authority to deny authorizations for all Hikvision equipment, irrespective of where it is deployed, its function, or its purpose. But that effort must fail because it is inconsistent with the specific distinctions drawn by Congress in restricting government funding or use of Hikvision equipment only *for certain purposes*, leaving the vast majority of Hikvision’s products and end users unaffected. Congress’s fundamental intent underlying both statutes is unambiguous—while some specific uses of Hikvision equipment are prohibited, the remainder are permitted. The Commission has no authority to overturn that congressional determination, and certainly those limited restrictions cannot expand the Commission’s authority by implication.

But that is the practical effect of the NPRM’s proposed rule. On the one hand, the Commission acknowledges that its proposed broad ban is “not specifically authorized by the

⁶⁶ *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Second Report and Order, 35 FCC Rcd. 14284, 14300 ¶ 33 (2020) (“*Supply Chain Second Report and Order*”).

⁶⁷ 2019 NDAA § 889, 132 Stat. at 1917.

⁶⁸ 47 U.S.C. § 1601.

Secure Networks Act itself, pursuant to which the Commission adopted the Covered List.”⁶⁹ At the same time, however, the Commission claims that to “effectively preclude use of equipment on the Covered List by USF recipients as contemplated by Congress, it is necessary . . . to restrict further equipment authorization . . . of such devices in the first instance.”⁷⁰ But that ignores the distinctions drawn by Congress, as well as the Commission’s own implementation of them.

In section 889(f)(3)(A), Congress indicated that *all* “[t]elecommunications equipment or services” manufactured by Huawei and ZTE should be included on the Covered List and thus prohibited from the United States’ market.⁷¹ But as to the other manufacturers, including Hikvision, the Commission found that Congress intended that equipment should be placed on the covered list only “to the extent it is used for public safety or security”⁷² and “capable of the functions outlined in sections 2(b)(2)(A), (B), or (C) of the Secure Networks Act.”⁷³ The Commission accordingly also found that its remove-and-replace requirement for USF recipients should be “narrowly tailored” to a “risk-based assessment of problematic equipment and services, consistent with the approach taken in section 889.”⁷⁴ Requiring removal of “all equipment and services from covered companies” would “risk[] being too broad and excessively burdensome.”⁷⁵ The *Supply Chain Second Report and Order* further explained that this is because “the Covered List is limited” to equipment and services “that are placed at the most

⁶⁹ *Covered Equipment NPRM* ¶ 65.

⁷⁰ *Id.*

⁷¹ 2019 NDAA § 889(f)(3)(A).

⁷² *See Supply Chain Second Report and Order* ¶ 68; 2019 NDAA § 889(f)(3)(B).

⁷³ *See Supply Chain Second Report and Order* ¶ 68.

⁷⁴ *Id.* ¶ 33.

⁷⁵ *Id.*

vulnerable spots in our communications infrastructure.”⁷⁶ Plainly, Hikvision equipment used by private companies to ensure the security of their physical premises are not “placed at the most vulnerable spots” in our communications infrastructure. The NPRM offers no reasoned explanation for departing from these recent findings by the Commission.⁷⁷

It bears emphasis, moreover, that with respect to Hikvision, it is an enormous understatement to say that its equipment is not used at the “most vulnerable spots” in the communications infrastructure. Hikvision equipment is not telecommunications equipment at all, as that term is defined in the Communications Act. Again, section 889 specifically targets certain “telecommunications equipment or services.”⁷⁸ The term “telecommunications equipment” generally means “equipment, *other than customer premises equipment*, used by a carrier to provide telecommunications services, and includes software integral to such equipment (including upgrades).”⁷⁹ But Hikvision equipment *is* “customer premises equipment,” and it is *not* “used by a carrier to provide telecommunications services.” Of course, section 889(f)(3)(B) expands the usual definition of “telecommunications equipment” to include

⁷⁶ *Id.*

⁷⁷ Section 889 also cannot be a basis for adopting the proposed ban on Hikvision equipment because it is an unconstitutional bill of attainder. Bills of attainder are “legislative punishment, of any form or severity, of specifically designated persons or groups.” *United States v. Brown*, 381 U.S. 437, 447 (1965). Section 889 specifically names Hikvision. The question is accordingly whether it imposes punishment. It does. Without due process or explanation, Congress blacklisted Hikvision in the United States. Moreover, Hikvision’s original listing in section 889 came with no notice, no public presentation of any evidence that it posed a national security threat, no application of general, scientific standards, no public hearing, no opportunity for Hikvision to challenge the listing or learn or rebut any information upon which the listing was based, and no formal process by which Hikvision could mitigate or be eventually removed from the list. The Bill of Attainder Clause prevents Congress from imposing a punishment as sweeping as a complete ban from the market on specific individuals or corporations.

⁷⁸ *See, e.g.*, 2019 NDAA § 889(a)(1)(A).

⁷⁹ 47 U.S.C. § 153(52) (emphasis added).

“video surveillance . . . equipment produced by . . . Hikvision,” but *only to the extent* that it is used “[f]or the purposes of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes.” The vast majority of Hikvision surveillance equipment—which is used by private companies on private premises that are not critical infrastructure—thus is *not* “telecommunications equipment” and *not* covered by section 889. Indeed, the General Services Administration has clarified in a decision tree provided to government contractors that the prohibition of section 889 only applies to Hikvision equipment if and only if their equipment is used for public safety, security of government facilities, physical security surveillance of critical infrastructure, or other national security purposes. If the answer to that use question is “no,” then the Hikvision equipment on the contractor’s supply chain is *not* covered by section 889.⁸⁰ This contrasts with the decision tree

⁸⁰ U.S. Gen. Servs. Admin. SCRM Rev. Bd., *SCRM Criteria for Section 889 Part B*, at 1 (Aug. 13, 2020), https://www.gsa.gov/cdnstatic/SCRM%20review%20board%20889%20PART%20B%20Rubric_0.pdf, provides:

3. Is the equipment identified by the offeror/contractor covered? - If you are only reviewing a telecommunications service, skip section 3 and go to section 4 of the rubric.
 - a. Is the answer to any of the following “Yes”?
 - i. Per (f)(3)(A) of Section 889 - Is the equipment telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation or a subsidiary or affiliate of either?
 - ii. Per (f)(3)(B) of Section 889 - Is the equipment video surveillance and telecommunication equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company or a subsidiary or affiliate AND do any of the following purposes of the use of technology apply?
 1. Public Safety?
 2. Security of Government facilities?
 3. Physical security surveillance of critical infrastructure?
 4. Other National Security Purposes
 - iii. Is the equipment covered?

for Huawei and ZTE equipment, which asks contractors only to determine whether the equipment is produced by Huawei or ZTE and does not add any additional use requirement for the prohibition of section 889 to apply.

In the same way, the NPRM conflicts with the Covered List itself, on which the NPRM depends. The Commission proposes to deny authorization to “[a]ny equipment on the Covered List.”⁸¹ But Hikvision equipment is on the Covered List *only* “to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes,” which is a device-by-device question. Thus, a particular Hikvision model can both be “on” and not “on” the Covered List at the same time, depending on how individual devices are used. It is thus impossible to deny authorization *ex ante* to all Hikvision “equipment on the Covered List.”

The NPRM’s proposed ban on Hikvision equipment authorizations is also inconsistent with the SNA. The SNA’s section (b)(2) limits the “communications equipment” the Commission should place on the Covered List to that capable of specific functions—such equipment must be “capable” of “routing or redirecting user data traffic or permitting visibility into any user data or packets;” “causing the network of a provider of advanced communications service to be disrupted remotely;” or “otherwise posing an unacceptable risk to the national security of the United States.”⁸² SNA’s section (b)(2) thus mirrors section 889(a)(2)(B), which

-
1. If the answer to both 3(a)(i) and 3(a)(ii) of the rubric is No, STOP -
- Prohibition under Part B does not apply.
 2. If the answer to either 3(a)(i) or 3(a)(ii) of the rubric is Yes,
continue through the rubric to determine if Prohibition under Part
B applies.

⁸¹ *Covered Equipment NPRM*, app. A.

⁸² 47 U.S.C. § 1601(b)(2); 47 C.F.R. § 1.50002; *see also Covered Equipment NPRM* ¶ 37 n.126 (“[W]here equipment or services on the list are identified by category, such category should

provides that the NDAA’s prohibitions do *not* “cover telecommunications equipment that *cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.*”⁸³ The SNA further defines the term “communications equipment or service” to mean “any equipment or service that is essential to the provision of advanced communications service,”⁸⁴ where “advanced communications service” means any “high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology.”⁸⁵ In the *Supply Chain Second Report and Order*, the Commission interpreted the phrase “communications equipment or services” to include “all equipment or services used *in* fixed and mobile broadband networks, provided they include or use electronic components.”⁸⁶ The Commission gave examples of such equipment, including “optical switching equipment” and “software and firmware used in broadband networks.”⁸⁷

The Hikvision equipment representing the vast majority of sales in the United States—the company’s cameras and recorders discussed *supra* at Part II.A—does not fall within any of these definitions. First, those devices do not “route or redirect user data traffic or permit visibility into any user data or packets.” Indeed, when cameras and recorders are deployed in a standalone video surveillance installation, by definition they cannot route or redirect user data traffic or

be construed to include only equipment or services capable of the functions outlined in sections 2(b)(2)(A), (B), or (C) of the Secure Networks Act.”).

⁸³ 2019 NDAA § 889(a)(2)(B) (emphasis added).

⁸⁴ 47 U.S.C. § 1608(5).

⁸⁵ 47 U.S.C. § 1302(d).

⁸⁶ *Supply Chain Second Report and Order* ¶ 52 (emphasis added). This definition conflicts with the statutory scheme because it erases the limiting phrase “essential to” in § 1608(5) by sweeping in all in-network equipment with electronic components.

⁸⁷ *Id.* ¶ 52 n.161.

permit visibility into any user data or packets. But even when used in conjunction with a LAN, Hikvision cameras do not “route” traffic—they simply generate video signals, much as a musical instrument generates audio signals. Neither a camera nor a musical instrument “routes” the signal it produces. Second, Hikvision cameras are not “used in” broadband networks: Unlike optical equipment or network software, but like a laptop, they *connect to* such networks at the periphery; they are not themselves “essential” to the provision of any telecommunications capability. The music analogy again applies. An electric guitar, for example, *connects to* a PA system but is not “used in” the PA system. Again, the guitar generates a signal carried by the system, much as a camera generates a signal carried by the network to which it connects. Finally, much the same is true of Hikvision video recorders—like a tape deck or a disc player in an audio system, video recorders *record* and *play* signals but do not “route” them. Such recorders, moreover, are not used *in* a broadband network, but merely provide data to be carried *by* the network.

In sum, under both the SNA and the NDAA, *Congress* has made the determination that there should *not* be a blanket ban on Hikvision equipment in the United States. These statutes provide no authority for such a ban—and, in fact, the NPRM’s proposals are inconsistent with the statutes because they obliterate Congress’s distinction among permissible and impermissible uses, and unreasonably depart from the Commission’s own previous recognition of that congressional boundary.

C. Title I Provides the Commission Neither Direct nor Ancillary Authority Over Devices like Hikvision Cameras and NVRs that Are Peripheral to the Communications Infrastructure.

As set forth above, neither Title III nor recent congressional enactments provide the Commission any express authority over CPE like Hikvision cameras and recorders. The NPRM,

however, also invokes provisions of Title I, including the Commission’s authority to “regulat[e] interstate and foreign commerce in communications by wire and radio”⁸⁸ and to adopt such rules “as may be necessary in the execution of its functions.”⁸⁹ But these provisions of Title I are not free-floating grants of jurisdiction—“Title I is not an independent source of regulatory authority.”⁹⁰ The Commission may only invoke its ancillary jurisdiction under Title I where two conditions are met: “(1) the Commission’s general jurisdictional grant under Title I covers the regulated subject and (2) the regulations are reasonably ancillary to the Commission’s effective performance of its statutorily mandated responsibilities.”⁹¹ The Commission’s efforts to invoke ancillary jurisdiction here fail both requirements.

D. The Commission’s General Jurisdictional Grant Under Title I Provides No Authority to Regulate Customer Premises Equipment that Is Peripheral to Communications Networks.

As discussed above, the primary categories of Hikvision equipment at issue here—cameras and video recording devices—are not the kinds of equipment used by carriers to provide communications services, but rather are used by private companies to ensure the security of their

⁸⁸ 47 U.S.C. § 151.

⁸⁹ *Id.* § 154(i). Title III also contains a similar broad authorization permitting “the Commission from time to time, as public convenience, interest, or necessity requires” to “[m]ake such rules and regulations and prescribe such restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of this chapter.” 47 U.S.C. § 303(r). This provision has the same limitations as the general jurisdictional grant of Title I, however—it must be tied to specific statutorily mandated responsibilities. *See also Huawei v. FCC*, No. 19-60896, 2021 WL 2493660, at *10 (5th Cir. 2021) (stating that “[w]e would be troubled if the FCC were trying to leverage its ‘public interest’ authority over networks into the power to make freewheeling national security judgments” and upholding the Commission’s ban on use of USF funds to buy Huawei equipment because it fell within the Commission’s express authority to define and establish universal service policies under Section 254).

⁹⁰ *People of the State of Cal. v. FCC*, 905 F.2d 1217, 1240 n.35 (9th Cir. 1990); *see also Mozilla Corp. v. FCC*, 940 F.3d 1, 76 (D.C. Cir. 2019).

⁹¹ *American Library Ass’n*, 406 F.3d at 691–92.

premises. They are thus paradigmatic CPE, as defined in the Communications Act.⁹² The courts have made clear that the Commission lacks general authority to regulate CPE outside of its use in interstate or foreign communications, and the Commission itself has long declined to do so as a matter of policy.

The D.C. Circuit’s decision in *American Library Ass’n* (“*ALA*”), illustrates why the proposals of the NPRM fail the first prong of the ancillary jurisdiction analysis. In *ALA*, the Commission sought to “regulate apparatus that can receive television broadcasts when those apparatus are not engaged in the process of receiving a broadcast transmission.”⁹³ Specifically, the Commission had required digital television reception devices to be manufactured with the capability to prevent unauthorized redistributions of digital content by recognizing a “broadcast flag” embedded in previously broadcast content.⁹⁴ The court noted that proponents of the regulation had, before the Commission, invoked both the Commission’s “express statutory authority”⁹⁵ under Title III to issue new licenses for advanced television services, and the Commission’s “ancillary jurisdiction” under Title I.⁹⁶

Before the D.C. Circuit, however, the Commission did not rely on Title III, presumably because opponents had pointed out “that the plain text of § 336 authorized the FCC to regulate only [digital television] broadcast licensees and the quality of the signal transmitted by such licensees,”⁹⁷ not the devices enabling receipt of digital transmissions. The court’s analysis

⁹² 47 U.S.C. § 153(16).

⁹³ *American Library Ass’n*, 406 F.3d at 691.

⁹⁴ *Id.*

⁹⁵ *Id.* at 694.

⁹⁶ *See* 47 U.S.C. § 336.

⁹⁷ *American Library Ass’n*, 406 F.3d at 694.

therefore focused on whether “the Commission’s general jurisdictional grant under Title I cover[ed] the subject of the regulations.”⁹⁸ In concluding that it did not, the court explained that “the agency’s general jurisdictional grant”—*i.e.*, Title I’s delegation of authority to the Commission to regulate “interstate and foreign communication by wire or radio”⁹⁹—“does not encompass the regulation of consumer products that can be used for receipt of wire or radio communication when those devices are not engaged” in such communications.¹⁰⁰ The court found that because the Commission’s order “impose[d] regulations on devices that receive communications” rather than “regulat[ing] the communications themselves,” the Commission had “exceeded the scope of its general jurisdictional grant under Title I.”¹⁰¹

A similar analysis applies here. As discussed in Part III.A, above, the provisions of sections 302 and 303 link the Commission’s regulatory authority to RF spectrum, emissions, and broadcasting—much as section 336 links the Commission’s authority to television *broadcasts*. And just as the general jurisdictional grant in Title I did not transform the Commission’s jurisdiction over television broadcasting into general authority to regulate “consumer products” used to receive broadcasts, Title I likewise does not transform the Commission’s authority over RF emissions and broadcasting into general authority to regulate CPE *unrelated* to its emissions.¹⁰² Yet that is what the Commission’s ban on importation and marketing would do—it would directly regulate the devices themselves, regardless of whether or how they are being used.

⁹⁸ *Id.* at 700.

⁹⁹ 47 U.S.C. § 152(a).

¹⁰⁰ *American Library Ass’n*, 406 F.3d at 700.

¹⁰¹ *Id.* at 703.

¹⁰² *Id.*

Notably, the Commission itself has also repeatedly held that CPE should remain unregulated. This principle dates back to the Commission’s *Carterfone* decision in the 1960s, which held that “interconnecting devices which do not adversely affect the telephone system” should generally be permitted.¹⁰³ In the 1970s and 1980s, in the *Computer Inquiry* decisions, the Commission further elaborated its deregulatory approach to CPE, finding, for example, that “CPE is a severable commodity from the provision of transmission services and that regulation of CPE under Title II is not required and is no longer warranted.”¹⁰⁴ And the Commission has repeatedly reaffirmed this approach in the Internet era, explaining that “[t]o encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to connect their choice of legal devices that do not harm the network.”¹⁰⁵ In sum, the Commission’s own treatment of CPE is consistent with the D.C. Circuit’s decision in *ALA*—the Commission has long disclaimed any general authority to regulate CPE. The Supreme Court has, moreover, found such a “disavowal of jurisdiction” directly relevant to the scope of an agency’s regulatory authority.¹⁰⁶ The Commission provides no analysis justifying its departure from this longstanding policy.

¹⁰³ See *Use of the Carterfone Device in Message Toll Telephone Service*, Decision, 13 FCC.2d 420, 423 (1968).

¹⁰⁴ *Amendment of Section 64702 of the Commission’s Rules and Regulations (Second Computer Inquiry)*, Final Decision, 77 FCC.2d 384, 388 ¶ 9 (1980).

¹⁰⁵ *Appropriate Framework for Broadband Access to the Internet Over Wireless Facilities*, 20 FCC Rcd. 14986, 14988 ¶ 4 (2005). Plainly Hikvision’s cameras and NVRs could not possibly harm any public network when operating on standalone internal networks. But even when connected to public WANs, there is no evidence that the security measures taken by Hikvision and its end users are in any way inadequate to guarding against outside threats.

¹⁰⁶ See *FDA v. Brown & Williamson*, 529 U.S. 120 (2000) (finding that the agency’s “disavowal of jurisdiction” and Congress’s legislation against that backdrop confirmed the agency’s lack of jurisdiction).

Significantly, when the Commission *has* previously regulated at-home Internet-of-Things devices, it has relied on a specific congressional grant of authority, not on Title I’s general jurisdictional grant. For instance, in establishing v-chip requirements, the Commission relied on section 551 of the 1996 Telecommunications Act, which, among other directives, required it to adopt rules to require certain television receivers to be equipped with v-chip technology to block certain types of programming based on its rating for violence, sex, and language.¹⁰⁷ Similarly, over the years, the Commission exercised its authority to require wireless phones and wireline telephones to be compatible with—and not to cause interference with—hearing aids, under the Hearing Aid Compatibility Act.¹⁰⁸ Congress expressly gave the Commission authority over “establish[ing] . . . regulations as are necessary to ensure reasonable access to telephone service by persons with impaired hearing,” and required that nearly all telephones manufactured in the United States or imported for use in the United States be hearing aid compatible as defined in the statute.¹⁰⁹ In adopting device accessibility regulations, the Commission has also acted upon the authority granted to it by Congress in the Twenty-First Century Communications and Video Accessibility Act (“CVAA”).¹¹⁰ Again, these are all *express* grants of specific regulatory authority and do not suggest that the Commission has any general authority over CPE under Title I.

¹⁰⁷ See *Implementation of Section 551 of the Telecommunications Act of 1996 Video Programming Ratings*, Report and Order, 13 FCC Rcd. 8232 (1998).

¹⁰⁸ Hearing Aid Compatibility Act of 1988, Pub. L. No. 100-394, 102 Stat. 976 (1988), codified as 47 U.S.C. § 610.

¹⁰⁹ See *id.*

¹¹⁰ See Twenty-First Century Communications and Video Accessibility Act of 2010, Pub. L. No. 111-265, 124 Stat. 2795 (2010) (making technical corrections to the CVAA); H.R. Rep. No. 111-563, at 19 (2010); S. Rep. No. 111-386 (2010).

E. The NPRM’s Proposed Ban on Hikvision Equipment Is Not “Reasonably Ancillary” to the Commission’s Effective Performance of Any Statutorily Mandated Responsibility.

Under the second prong of the ancillary jurisdiction analysis, the Commission must point to a specific statutory provision or provisions that the proposed regulations are *reasonably* ancillary to effectuating.¹¹¹ To demonstrate “reasonableness,” the Commission cannot merely point to one or more specific delegations of authority, but must also “establish” that the proposed regulations “will fulfill [the] specific statutory goal” and are “rational and supported by substantial evidence.”¹¹² Under this analysis, none of the specific statutory provisions the Commission cites in the NPRM are capable of sustaining the exercise of ancillary jurisdiction.

1. The Secure Networks Act provides no ancillary jurisdiction.

As set forth above, and as the NPRM acknowledges, the SNA directs the Commission to prevent federal subsidies that it administers from being used to acquire or maintain equipment on the covered list but does not “specifically authorize[]” the proposed rules.¹¹³ The Commission suggests that the rules are still necessary to “effectively preclude use of equipment on the Covered List by USF recipients as contemplated by Congress.”¹¹⁴ But that is simply not so—barring *all* importation of Hikvision equipment is neither *reasonably* ancillary to ensuring that it is not acquired with USF subsidies nor supported by substantial evidence.

¹¹¹ See *Comcast Corp. v. FCC*, 600 F.3d 642, 653 (D.C. Cir. 2010) (quoting *NARUC v. FCC*, 533 F.2d 601, 612 (D.C. Cir. 1976)) (ancillary authority is “incidental to, and contingent upon, *specifically delegated powers under the Act*”); see also *Motion Picture Ass’n of Am. v. FCC*, 309 F.3d 796, 806–807 (D.C. Cir. 2002) (rejecting the Commission’s “argument that [its] video description rules are obviously a valid communications policy goal and in the public interest” because the Commission “can point to no statutory provision that gives the agency authority” to issue those rules).

¹¹² *Verizon v. FCC*, 740 F.3d 623, 644 (D.C. Cir. 2014).

¹¹³ *Covered Equipment NPRM* ¶ 65.

¹¹⁴ *Id.*

A broad ban on Hikvision equipment—*i.e.*, “restrict[ing] further equipment authorization”¹¹⁵—is drastically overbroad if the Commission’s goal is to prevent USF funds from being spent improperly.¹¹⁶ The Commission routinely ensures that USF money is only spent on eligible products or services without banning ineligible products from the country altogether. For example, E-Rate funds are only available for specifically listed services and products to help schools and libraries obtain affordable broadband,¹¹⁷ and many devices and services on the market are thus not E-Rate eligible. With respect to each of these programs, the Commission does not ban ineligible equipment that has uses for other purposes. Instead, the Commission reasonably employs more limited steps: It requires E-Rate recipients to submit certifications, and it empowers the Universal Service Administrative Company to audit USF receipts to detect waste, fraud, and abuse. It was unreasonable for the Commission to fail to take such a measured approach here.

That is particularly true given that 1) there is very little Hikvision equipment that would be eligible for USF support; and 2) the Commission advances no evidence to suggest that any Hikvision equipment has ever been improperly reimbursed even absent the draconian ban in the NPRM. With respect to the first point, Hikvision cameras and recorders would certainly not fall within the equipment covered by the E-rate Category Two list,¹¹⁸ nor would they be covered by

¹¹⁵ *Id.*

¹¹⁶ The SNA’s other stated objectives are not even plausibly related to the proposed rules.

¹¹⁷ See *Modernizing the E-Rate Program for Schools and Libraries*, Order, 35 FCC Rcd. 13793, 13799–805 app. B (2020) (publishing list of authorized services and equipment).

¹¹⁸ See *id.* (eligible equipment includes antennas, connectors, and related components used for internal broadband connections; cabling; racks; routers; switches; Uninterruptible Power Supply (UPS)/Battery Backup; access points used in a LAN or WLAN environment (such as wireless access points); wireless controller systems; and software supporting the components

Rural Health Care or Lifeline support mechanisms.¹¹⁹ And while it is at least possible that site security for a high-cost, rate-of-return telecommunications company might be eligible for USF reimbursement—that is a very limited application that could be readily policed by rule and is already the subject of the SNA. With respect to the second point, under its ancillary jurisdiction, the Commission may not merely invoke a specific statutory responsibility but must also demonstrate that it is not tilting at windmills—it must establish that the proposed rule is supported by “substantial evidence.”¹²⁰ The Commission cannot do so here—again, Hikvision is aware of *no* evidence that its products have ever been improperly reimbursed under the USF Program. Because the NPRM’s proposals are not reasonably ancillary to effectuating the ban on federal subsidies, there is no ancillary jurisdiction under the SNA.

on this list used to distribute high-speed broadband throughout school buildings and libraries). The E-Rate Category One list is limited to eligible services. *Id.*

¹¹⁹ The Lifeline Program provides a federal subsidy for network access for one line—either a landline or wireless/mobile option—per eligible household and does not provide a subsidy for devices (*i.e.*, handsets or CPE). *Lifeline and Link Up Reform and Modernization; Telecommunications Carriers Eligible for Universal Service Support; Connect America Fund*, Third Report and Order, Further Report and Order, and Order on Reconsideration, 31 FCC Rcd. 3962, 4005 ¶ 125 (2016). The Rural Health Care Program comprises both the Healthcare Connect Fund Program and the Telecommunications Program. The Healthcare Connect Fund Program provides support for high-capacity broadband connectivity to eligible health care providers and encourages the formation of state and regional broadband health care provider networks. *See Rural Health Care Support Mechanism*, Report and Order, 27 FCC Rcd. 16678, 16681 ¶ 1–3 (2012). Under the Rural Health Care Program, eligible rural health care providers can either receive a subsidy for telecommunications services to reduce them to urban levels, or, along with those eligible non-rural health care providers that are members of a consortium that has more than 50% rural health care provider sites, receive a 65% flat discount on an array of communications services, including both telecommunications and internet access. Under the latter option, these services include internet access, dark fiber, business data, traditional DSL, and private carriage services, but do not extend to security devices or services. *Id.*; *Healthcare Connect Fund – Frequently Asked Questions*, FCC, <https://www.fcc.gov/general/healthcare-connect-fund-frequently-asked-questions#Q1> (last revised Apr. 30, 2015).

¹²⁰ *Verizon*, 740 F.3d at 644.

Furthermore, if the goal of the NRPM is to “effectively preclude use of equipment on the Covered List by USF recipients as contemplated by Congress,”¹²¹ the Commission could have taken the less restrictive and more straightforward step of prohibiting USF recipients from using equipment on the covered list. Not only did it not take that more direct step, but in its recent *Supply Chain Third Report and Order*, the Commission made it clear that USF recipients will not be reimbursed to remove Hikvision equipment from their networks, and therefore do not have a legal obligation to remove Hikvision equipment either.¹²² This decision followed Congress’s own determination in the Consolidated Appropriations Act (“CAA”) to make reimbursement funds available only for the removal of Huawei and ZTE equipment—and not Hikvision equipment—evidently deeming the former a more pressing national security objective than the latter.¹²³ And lest it impose an unfunded mandate on commercial providers of advanced communications services, the Commission determined that there could be no legal obligation for providers or USF recipients to remove Hikvision equipment either.¹²⁴ But if the Commission and Congress do not deem the removal of Hikvision equipment from the networks of commercial providers of advanced communications networks to be a pressing national security objective sufficient to warrant reimbursement funds, and if providers and USF recipients do not therefore have a legal obligation to remove Hikvision equipment, then this justification for the NPRM as

¹²¹ *Covered Equipment NPRM* ¶ 65.

¹²² *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Third Report and Order, FCC 21-86, WC Docket No. 18-89, ¶¶ 18, 37 (rel. July 14, 2021) (“*Supply Chain Third Report and Order*”).

¹²³ Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, § 901, 134 Stat. 1182, 2120–21 (2020).

¹²⁴ *Supply Chain Third Report and Order* ¶¶ 38–39 (“The Commission made compliance with the remove-and-replace requirement contingent upon an appropriation from Congress to the Reimbursement Program.”).

applied to Hikvision dissolves. The Commission would be taking the greater step of banning the sale and marketing of all Hikvision equipment, and imposing huge costs on industry and small businesses, only to preclude USF recipients from using equipment which the Commission has said they are not even required to remove. And instead of imposing an unfunded mandate on large, sophisticated providers of advanced communications, the Commission would effectively impose a much costlier unfunded mandate on thousands of small businesses to remove Hikvision from their networks, with no discernible national security justification.

2. *Section 302, section 303, and other statutory provisions imposing responsibilities relating to RF spectrum and interference provide no ancillary jurisdiction under Title I.*

The Commission invokes a number of provisions of Title III and other statutes that confer responsibilities on it relating to managing the RF spectrum and interference. But the NPRM's proposed ban is not reasonably ancillary to fulfilling the Commission's spectrum management responsibilities and indeed bears no rational relationship to managing the RF spectrum or interference within it.

As set forth in Part III.A, above, Title III gives the Commission express authority to “manage spectrum . . . in the public interest.”¹²⁵ But the NPRM's proposed limitations on importation, marketing, and use have nothing to do with managing the RF spectrum—they would instead limit the ability to bring Hikvision *devices* into the United States. As also discussed above, sections 302 and 303 are not about regulating *devices* generally. Those provisions tie the Commission's regulatory authority to managing the RF spectrum and

¹²⁵ *Cellco*, 700 F.3d at 541 (quoting *Reexamination of Roaming Obligations of Commercial Mobile Radio Serv. Providers & Other Providers of Mobile Data Servs.*, Second Report and Order, 26 FCC Rcd. 5411, 5440 ¶ 62 (2011)).

interference.¹²⁶ But Hikvision’s security cameras and recorders are largely interchangeable with those of other manufacturers. They pose no unique problems with respect to the RF problem—and, indeed, no problems at all, since they entirely conform to the Commission’s regulatory requirements. The NPRM’s proposed ban on Hikvision *devices* is thus not even rationally related to the Commission’s authority over spectrum and spectrum interference, and certainly such a ban is not an “ancillary” *requirement* of spectrum regulation.

In addition to provisions of Title III, the NPRM also cites a handful of other statutory sources of authority to RF interference as potential justifications for the proposed ban. Those provisions include the Commission’s authority to address human RF exposure under the National Environmental Policy Act¹²⁷ and its responsibility to ensure compatibility between mobile handsets and hearing aids.¹²⁸ Plainly, however, banning Hikvision devices has nothing to do with the Commission’s jurisdiction in either regard, and those provisions are thus simply irrelevant.

3. *CALEA provides no ancillary jurisdiction.*

The NPRM also invokes CALEA as a potential source of authority. Section 105 of CALEA does address telecommunications system security and integrity; it requires telecommunications carriers to ensure that the surveillance capabilities built into their networks “can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance

¹²⁶ See *supra* at Part III.A.

¹²⁷ See 47 C.F.R. §§ 2.1091–1093.

¹²⁸ See 47 U.S.C. § 610.

with regulations prescribed by the Commission.”¹²⁹ At the same time, however, CALEA applies only to network equipment, not CPE—specifically, CALEA applies to the “equipment, facilities, or services” of a “telecommunications carrier” that “provide a customer or subscriber with the ability to originate, terminate, or direct communications.”¹³⁰ The Commission does not and cannot explain how the proposed regulations barring Hikvision cameras and recorders could be reasonably ancillary to ensuring the security of network equipment and facilities under CALEA, and plainly they are not.

IV. THE PROPOSED REGULATIONS WOULD BE ARBITRARY AND CAPRICIOUS.

In addition to exceeding congressional delegations of authority to the Commission, the proposals of the NPRM are arbitrary and capricious—the Commission proposes to single out Hikvision equipment on grounds that are impossible to square with reasoned decision making. As noted above, Hikvision does not provide network equipment. Its cameras and NVRs are peripheral devices—not telecommunications equipment used by carriers in network infrastructure—and keeping American businesses from using Hikvision equipment in their security systems will not enhance the security of the nation’s telecommunications networks.

There is, moreover, no “satisfactory explanation” for the Commission to reverse its longstanding deregulatory policy with respect to end user devices.¹³¹ Targeting Hikvision and other individual companies’ CPE through the Commission’s proposed equipment authorization

¹²⁹ 47 U.S.C. § 1004.

¹³⁰ 47 U.S.C. § 1002(a); *see generally Communications Assistance for Law Enforcement Act (CALEA) and Broadband Access and Services*, First Report and Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd. 14989 (2005).

¹³¹ *Motor Vehicle Mfrs. Ass’n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983).

rules is arbitrary and capricious because it would (1) treat similar companies and products differently; (2) rely on factors that Congress did not intend to be considered when setting equipment authorization criteria and fail to consider less restrictive alternatives; (3) address hypothetical scenarios, not demonstrated problems; and (4) have an adverse effect on global trade and American businesses.

A. The Proposed Regulations Are Arbitrary and Capricious Because They Would Treat Similar Companies and Products Differently.

The courts of appeals have “long held that an agency must provide adequate explanation before it treats similarly situated parties differently.”¹³² But the NPRM focuses on Hikvision and other individual companies rather than adopting generally applicable criteria applicable to all similarly situated companies.¹³³ The NPRM thus represents an “individual action” that is, at best, barely “masquerading as a general rule.”¹³⁴ In reality, Hikvision poses no greater threat—and arguably far less of a threat—than companies selling other, more vulnerable networkable equipment, or even Hikvision’s competitors selling other video surveillance equipment in the United States.

First, as noted above, security cameras and recorders generally pose far *less* of a national security threat to communications networks than a vast array of equipment that the Commission does not propose to regulate at all. Again, servers, switches, routers, and even the many millions

¹³² *Petroleum Commc’ns, Inc. v. FCC*, 22 F.3d 1164, 1172 (D.C. Cir. 1994); *see also New Orleans Channel 20, Inc. v. FCC*, 830 F.2d 361, 366 (D.C. Cir. 1987); *Pub. Media Ctr. v. FCC*, 587 F.2d 1322, 1331 (D.C. Cir. 1978); *Melody Music, Inc. v. FCC*, 345 F.2d 730, 732–33 (D.C. Cir. 1965).

¹³³ *Compare Comm. for Effective Cellular Rules v. FCC*, 53 F.3d 1309, 1319 (D.C. Cir. 1995) (finding that “the Commission did not choose among contenders for a particular license . . . but rather revised the technical specifications for *all* cellular licenses”).

¹³⁴ *Am. Airlines, Inc. v. Civil Aeronautics Bd.*, 359 F.2d 624, 631 (D.C. Cir. 1966).

of computers that connect to the Internet are all more integrated into communications networks than security cameras and video storage devices. Yet the Commission does not propose to regulate any of those devices, nor does it attempt to explain why surveillance equipment is of particular concern, particularly outside of the governmental sites already covered by section 889.

Second, within the realm of video surveillance equipment, Hikvision has demonstrated either significantly fewer or certainly no more vulnerabilities compared to other leading video surveillance manufacturers. There are no significant differences in cybersecurity practices between Hikvision and other manufacturers in the United States, and the Commission has not yet supported its different treatment of Hikvision.¹³⁵ The Common Vulnerabilities List (“CVE”), a library that tracks cybersecurity vulnerabilities and exposures launched by the MITRE Corporation and sponsored by the DHS Cybersecurity and Infrastructure Security Agency (“CISA”), reports one vulnerability in Hikvision video surveillance equipment to date in 2021, and found only one vulnerability in 2020, no vulnerabilities in 2019, and two vulnerabilities in 2018.¹³⁶ In fact, since 2015, CVE has reported only fifteen total vulnerabilities in Hikvision video surveillance equipment, with the majority of those occurring prior to 2015.¹³⁷ Further,

¹³⁵ See *Melody Music*, 345 F.2d at 732–33 (stating that “the Commission’s refusal to explain its different treatment of appellant and NBC was error” and “the differences are not so ‘obvious’ as to remove the need for explanation”); see also Comments of M&P Security Solutions LLC, ET Docket No. 21-232 (filed Sept. 1, 2021) (“M&P Security Solutions Comments”) (“As a Veteran Owned company, we fully agree with putting pressure on certain foreign country’s when it is warranted, including China. However, this specific FCC proposal seems more directly targeted at certain companies (including Hikvision) without a justifiable cause.”).

¹³⁶ See Hikvision Common Vulnerabilities and Exposures, CVE, <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Hikvision> (last visited Sept. 22, 2021).

¹³⁷ See *id.*

CVE has categorized only several of those fifteen vulnerabilities as critical and has not yet characterized the 2021 vulnerability as of the time of this filing.¹³⁸

Even though other video surveillance companies have vulnerability records similar to or greater than that of Hikvision's, they would not be subject to the Commission's proposed equipment authorization rules. The Commission has not explained—and cannot explain—why Hikvision's equipment poses a unique security threat.

B. The Commission Relies on Factors Congress Did Not Intend It to Consider When Setting Equipment Authorization Criteria and Fails to Consider Less Restrictive Alternatives.

As discussed in Part III.A, above, Congress clearly intended the Commission to consider two specific factors when setting RF equipment authorizations: interference potential and susceptibility to interference.¹³⁹ Plainly, an equipment's placement on a list of "covered entities" has no relation to either factor. Instead, the Commission appears to be considering perceived network security factors as a basis for denying, or rescinding, equipment authorizations. Thus, the Commission's proposed rules would rely on factors Congress did not intend the Commission to consider. This is arbitrary and capricious.¹⁴⁰ Further, an agency also acts arbitrarily and capriciously when it "fail[s] to consider an obvious and less drastic alternative" to its proposed policy.¹⁴¹ Yet the NPRM fails to demonstrate why less-drastic alternatives are inadequate to address any security concerns the Commission may have—even

¹³⁸ *See id.*

¹³⁹ 47 U.S.C. § 302a(a).

¹⁴⁰ *Motor Vehicle Mfrs. Ass'n*, 463 U.S. at 43 ("Normally, an agency rule would be arbitrary and capricious if the agency has relied on factors which Congress has not intended it to consider").

¹⁴¹ *Yakima Valley Cablevision, Inc. v. FCC*, 794 F.2d 737, 746 (D.C. Cir. 1986); *see also Edison Elec. Inst. v. EPA*, 2 F.3d 438, 448 (D.C. Cir. 1993) ("The failure to consider legitimate alternatives may render an agency decision arbitrary and capricious.").

putting aside the fact that such concerns are beyond Congress's delegation of authority to the Commission.

C. The Proposed Regulations Are Arbitrary and Capricious Because They Address Highly Speculative, Unsubstantiated Security Risks, not Demonstrated Problems.

Agencies must regulate on the basis of demonstrated problems, not hypothetical problems.¹⁴² However, in proposing its equipment authorization rules, the Commission appears to be targeting individual companies on the basis of speculative, unsubstantiated security fears rather than demonstrated problems. The Commission's concerns regarding Hikvision video surveillance equipment sold in the United States make little sense given the real-life ways in which Hikvision video surveillance equipment is used and the steps that IT administrators routinely take to secure their networks.¹⁴³ The Commission also fails to recognize Hikvision's exemplary record at identifying and addressing equipment vulnerabilities in a transparent manner and its commitment to resolving its equipment vulnerabilities, as well as its numerous efforts to ensure the security of its equipment and serve as a cybersecurity resource for its partners and end users.

Hikvision equipment is secure as deployed. Although the NPRM provides little information in this regard, unfounded fears of espionage or third-party access to Hikvision equipment appear to be driving the proposed rules to at least some degree. Yet such fears are implausible given the reality of how Hikvision video surveillance equipment is installed and used by end-users. As set forth above in Part II.A, Hikvision cameras are commonly deployed

¹⁴² See *Sorenson Commc'ns. Inc. v. FCC*, 755 F.3d 702,708 (D.C. Cir. 2014); *In re Permian Basin Area Rate Cases*, 390 U.S. 747, 792 (1968) (“[E]ach of the order’s essential elements [must be] supported by substantial evidence.”).

¹⁴³ See *supra* at Part II.A (discussing end user deployment of Hikvision products).

so as to be either physically or logically isolated from Internet-connected devices. In such deployments, security equipment either has no interface with outside networks, or enterprise-level security measures, such as firewalls, govern the extent to which the camera's network can communicate with outside networks. Indeed, multiple sellers of Hikvision products, including security business owners, confirm that the cameras are secured by a closed network, so that they never have direct access to the Internet.¹⁴⁴ Such physically or logically isolated deployments not only prevent inbound cybersecurity attacks, but also guard against outbound transmission. Further, even in the rare case of an Internet-connected deployment, an installer would likely set up a firewall between its network and the Internet, which can also be configured with intrusion detection functionality to read incoming packets, detect potentially suspicious or problematic data, and flag unauthorized attempted inbound data. An installer can also set up access control list rules at a firewall that restrict *any* attempted outbound transmission of data from the cameras and NVR, and permit such outbound transmission *only* from certain secure devices.

The president of Homeland Surveillance, Investigations & Installations—which to date has installed and maintained over sixty thousand cameras in New York City and the surrounding areas—explains that in order to penetrate such a closed network, an intruder would require the

¹⁴⁴ See, e.g., Comments of Ben Brooks, ET Docket No. 21-232 (filed Aug. 27, 2021) (“Brooks Comments”) (stating that an installer would “never have a CCTV system directly connected to the [I]nternet” because “that would be stupid”); Comments of Shane Nevins, ET Docket No. 21-232 (filed Aug. 24, 2021) (“Nevins Comments”) (stating that his company has “always been diligent in segmenting our networks so that our cameras never have direct access to the internet” and provides “a remote connection to [its] clients, but always through an intermediate interface”); Comments of Kyle Folger, ET Docket No. 21-232 (filed Aug. 27, 2021) (“Folger Comments”) (“Many of the systems are using the cameras on an isolated network not connected to the internet.”).

“IP [a]ddress,” the “port [n]umber,” the “user ID,” and the “password.”¹⁴⁵ While this company has secured many schools and residential and office complexes, and would be the first to be notified about a security breach, it has “never been notified about a security breach in any of [its] more than 1,000 systems deployed.”¹⁴⁶

Hikvision identifies and addresses vulnerabilities and has received high-level security certifications. As discussed in Part II.D, Hikvision has a stellar record of identifying and addressing security vulnerabilities in a transparent manner.¹⁴⁷ Again, prior to implementation and release to the public, Hikvision software undergoes extensive testing, including searching for known and unknown vulnerabilities, and any vulnerabilities exposed are patched by the software developer. Hikvision also continues to address vulnerabilities reported by the public after release, creating patches and making them directly available to end users. For example, in March 2017 a security researcher found and reported a vulnerability, and within six days, Hikvision released a firmware patch, notified its partners through a special bulletin, and notified the public with a notice on its website.

¹⁴⁵ Comments of Yisrael Gold, ET Docket No. 21-232 (filed Aug. 24, 2021) (“Gold Comments”) (Gold serves as president of Homeland Surveillance, Investigations & Intelligence Corp.).

¹⁴⁶ *Id.*

¹⁴⁷ *See, e.g.*, Comments of Andrew J. Staves, ET Docket No. 21-232 (filed Sept. 9, 2021) (“Over the past years Hikvision has made security changes to make their products more secure. Complex password requirements, a secure password reset system, and cloud based remote access all help secure their products.”); Comments of Don Richter, ET Docket No. 21-232 (filed Sept. 8, 2021) (stating that Hikvision is “responsive in issuing firmware upgrade to their products as needed not only to improve their products but to increase defense against cybersecurity threats”); M&P Security Solutions Comments (“Through the years, Hikvision has made firmware updates easier than ever to apply and has won many cybersecurity-related accolades and awards for their levels of encryption.”); Comments of Heather Martin, ET Docket No. 21-232 (filed Aug. 30, 2021) (listing Hikvision’s numerous cybersecurity accomplishments and efforts).

Hikvision has also taken seriously its responsibility to serve as a cybersecurity resource for its partners and end users, investing extensively in developing an array of scanning tools, unknown-vulnerability discovery tools, and network security hardening resources and best practices to help safeguard end users' systems. As a security professional stated in this docket, "Most surveillance systems are subject to a data breach no matter what you could do to prevent access to the video data, but the robust security structure in the Hikvision products limits the chance of any data breach."¹⁴⁸

Again, Hikvision also engages with third-party cybersecurity certifiers to test its products and has received numerous high-level cybersecurity certifications and recognitions. For some certifications, the testing process can take several months and requires multiple rounds of testing. Part II.F, *supra*, sets forth in greater detail Hikvision's extensive commitment to seeking and obtaining respected security certifications both in the United States and around the world.

Fears of Chinese intervention are unfounded. Concerns about Chinese government intervention in Hikvision video surveillance equipment are misplaced. First, shareholder CETC, a Chinese state-owned enterprise, is not involved in the day-to-day operations of the company. Second, even if the Chinese state-owned enterprise did exert substantial influence over Hikvision, there would be no threat to American businesses and consumers as, again, end users in the United States deploy Hikvision's devices so that they are physically or logically isolated from telecommunications networks, or in an Internet-connected deployment, are protected using VLANs and firewalls. Such installations are typically designed and monitored by the users' IT professionals to maintain security. Third, Hikvision generally does not know who its end users are or where they have located Hikvision equipment. In the United States, Hikvision sells

¹⁴⁸ Comments of William Bew, ET Docket No. 21-232 (filed Aug. 30, 2021).

through a network of distributors and dealers. The dealers are the ones that work with the end users and know who they are. Hikvision does not have a general warranty registration program or other program to collect information on specific end users, and its warranties all run through its dealers.

It also bears reemphasis that video streams from Hikvision cameras are all encrypted. It therefore makes little sense that these devices could serve as vectors for intrusive surveillance or initiate transmission of information.¹⁴⁹ As an Illinois-based security professional and seller of Hikvision video surveillance equipment states, to even access camera data, a Chinese hacker would have the challenging task of penetrating a “firewall, sometimes [two] firewalls, and somehow hide the exfiltration of an HD video stream or a still image” without being detected.¹⁵⁰ It is an unlikely scenario and one for which the Commission has provided no credible support, other than mere conjecture. And any hypothetical threat from Hikvision itself—of which, again, there has never been any evidence—is also limited by the fact that it is not a carrier exchanging traffic with other carriers, nor does it interconnect with a carrier signaling system, nor does it control how its equipment is interconnected with public networks, in the minority of situations in which that occurs.¹⁵¹

¹⁴⁹ Brooks Comments (“[I]t would be close to impossible for [the Chinese government] to somehow sneak in a piece of software or hardware that allows [it] to remotely access the [Hikvision] devices.”); Comments of Mark Zuckerman, ET Docket No. 21-232 (filed Sept. 9, 2021) (“Zuckerman Comments”) (“Based on best practices these systems run on a private network and should be nearly impossible to hack.”).

¹⁵⁰ Zuckerman Comments.

¹⁵¹ *Compare China Mobile International (USA) Inc.; Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended*, Memorandum Opinion and Order, 34 FCC Rcd. 3361, 3373–76 ¶¶ 24 n.76, 27-29 (2019) *with Covered Equipment NPRM*.

U.S. government officials and industry professionals agree that Hikvision equipment poses no national security threat. Finally, and notably, government officials, security professionals, and business owners throughout this country have acknowledged Hikvision’s efforts in cybersecurity and dispelled any notions that Hikvision’s video surveillance equipment poses a threat to the American telecommunications networks. Army Colonel Christopher Beck, Fort Leonard Wood’s Chief of Staff, firmly rejected the notion that the Army believed Hikvision cameras posed a security risk given their lack of Internet connection, stating, “We never believed [the cameras] were a security risk. They were always on a closed network.”¹⁵² Similarly, in response to questions in a January 2018 House Small Business Committee hearing about Hikvision equipment vulnerabilities, Richard Driggers, Deputy Assistant Secretary for the DHS Office of Cybersecurity and Communications, stated that once a vulnerability was discovered, “[w]e worked with [Hikvision]” and Hikvision “put out a software update that mitigated the impacts of this particular exploitation . . . [a] standard practice that we do at the Department of Homeland Security across many different companies’ devices and software.”¹⁵³ In addition, numerous American security professionals and business owners affirm that Hikvision equipment is secure, noting that Hikvision identifies and patches security issues that arise.¹⁵⁴ According to

¹⁵² Dan Strumpf, *Army Rips Out Chinese-Made Surveillance Cameras Overlooking U.S. Base*, WALL ST. J. (Jan. 12, 2018), <https://www.wsj.com/articles/army-rips-out-chinese-made-surveillance-cameras-overlooking-u-s-base-1515753001>.

¹⁵³ House Small Business Committee, *Small Business Information Sharing: Combating Foreign Cyber Threats*, YOUTUBE (Jan. 30, 2018), <https://www.youtube.com/watch?v=vWiBWkpVIAA&t=1575s>.

¹⁵⁴ See, e.g., M&P Security Solutions Comments (“We have never had any security-related issues with Hikvision equipment, specifically regarding hacking or any other cyber security threats.”); Comments of Safeguard Security Cameras, ET Docket No. 21-232 (filed Aug. 27, 2021) (“We have never once experienced any reason to question Hikvision USA’s commitment to protecting the US consumer market”); Comments of Michael Pittman, ET Docket No. 21-232 (filed Aug. 24, 2021) (“Pittman Comments”) (“Over the years

a North Carolina-based network engineer who sells and installs Hikvision cameras, there have never been any cybersecurity issues with the Hikvision equipment, and Hikvision has successfully passed many third-party security audits.¹⁵⁵ Notably, at the same time that the Commission proposed changes to its equipment authorization regime, President Biden revoked the previous administration’s executive order that sought to ban the popular apps TikTok and WeChat based on speculative threats, and replaced it with one that calls for the federal government to “evaluate” such apps and perceived national security threats from foreign-controlled apps “through rigorous, evidence-based analysis.”¹⁵⁶ The Commission should similarly avoid the pitfall of adopting rules based on hypothetical threat rather than demonstrated problems.

D. The Proposed Regulations Are Arbitrary and Capricious Because of the Highly Disruptive Effect They Would Have on American Businesses, Consumers, and Manufacturers Globally.

[Hikvision] ha[s] taken great lengths to increase security measures.”); Comments of Jerry De Francisco, ET Docket No. 21-232 (filed Aug. 20, 2021) (questioning the Commission’s factual basis for an equipment authorization ban on Hikvision video surveillance equipment); Comments of Aaron Oakley, ET Docket No. 21-232 (filed Aug. 19, 2021) (“Oakley Comments”) (“[W]e have gone to great lengths to test and find products that meet our standards of security, in all the time we have never had one single instance of any security issues described in the [Commission] proposal.”); Comments of Ron Valdez, ET Docket No. 21-232 (filed Aug. 24, 2021) (“Valdez Comments”); Brooks Comments; Comments of Martin VanConant, ET Docket No. 21-232 (filed Sept. 13, 2021) (stating that over ten years, his company has “installed hundreds of camera systems in our customer[s]’ homes and businesses that also haven’t had one issue of network vulnerability or cyber threats from the cameras having outside connectivity”); Comments of MyrtleNET, ET Docket No. 21-232 (filed Sept. 13, 2021) (stating that its over ten thousand Hikvision cameras are deployed with firewalls).

¹⁵⁵ Comments of Michael Bolton, ET Docket No. 21-232 (filed Aug. 27, 2021) (“Bolton Comments”).

¹⁵⁶ Exec. Order No. 14,034, 86 Fed. Reg. 31,423 (June 9, 2021), <https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries>.

Broad changes to the Commission’s equipment authorization regime would be highly disruptive and impose substantial burdens on American businesses, consumers, and manufacturers across the supply chain. That will both harm businesses and consumers by denying them access to reliable equipment to secure their premises in a cost-effective manner and will also impose strain on the global supply chain and interfere with global trade.

There is overwhelming consensus among security professionals across the country that the Commission’s proposed equipment authorization rules would have a catastrophic impact on American small security businesses and the consumers served by those businesses.¹⁵⁷ Hikvision offers secure, high-quality, and affordable video surveillance equipment. According to one

¹⁵⁷ See, e.g., Comments of Blue Sky Technologies LLC, ET Docket No. 21-232 (filed Aug. 25, 2021) (“Blue Sky Technologies Comments”) (“[B]anning the Hikvision line of camera systems in the United States would greatly impact not only [Blue Sky Technologies’] business and income, but also affect many of [its] clients who have spent hundreds of thousands of dollars on [Hikvision products].”); Comments of Guardian Safe & Lock LLC, ET Docket No. 21-232 (filed Aug. 30, 2021) (“Guardian Safe & Lock Comments”); Gold Comments (“My life, my employees[’] lives and thousands of other security installers and technicians will be severely impacted by disallowing us access to the world[’s] largest and most professional provider of security hardware.”); Bolton Comments (“Banning Hikvision products will be catastrophic for many businesses that are selling and installing [their] product It will also be catastrophic for the individuals that have systems now or need an affordable [security] system”); Oakley Comments (“[T]his FCC proposal could greatly affect my business, employees and our families.”); Pittman Comments (“The FCC proposal will hurt the small security businesses the most.”); Comments of Oscar Cortes, ET Docket No. 21-232 (filed Aug. 24, 2021) (“Cortes Comments”) (“Not allowing the sale of Hikvision products in the United States will directly impact the 24 families that depend on our company, as it is our primary line of products.”); Comments of Mike Hall, ET Docket No. 21-232 (filed Aug. 24, 2021) (“Hall Comments”) (“I feel if [the proposed rules are adopted] that there will be a lot of harm done to smaller contractors and installers that could and will impact our economy and the jobs market.”); Comments of Bob Ray, ET Docket No. 21-232 (filed Aug. 24, 2021) (“As a concerned reseller/certified installer[,] our business would drastically be impacted by not being able to secure and install Hikvision security product in the [U.S.] because of the large existing customer base that we maintain and support.”); Comments of Richard Rizzo, ET Docket No. 21-232 (filed Aug. 24, 2021); Valdez Comments; Zuckerman Comments; Comments of Junto Technology, LLC, ET Docket No. 21-232 (filed Sept. 13, 2021) (“Junto Technology Comments”) (stating that a ban on Hikvision equipment would “cause severe hardship on [its] company and its employees”).

Texas-based distributor, small security businesses “are only able to thrive because of companies like Hikvision,” which offer “good quality and price.”¹⁵⁸ Indeed, numerous distributors of Hikvision equipment agree that comparable video surveillance equipment on the market is significantly more expensive and less accessible to average American consumers seeking to protect their businesses or homes.¹⁵⁹ The elimination of Hikvision equipment from the U.S. market could result in the collapse of many small security businesses, with primarily large security companies left operating, to the detriment of American business owners and consumers.¹⁶⁰ Small security businesses also express concern that should the Commission adopt its proposed equipment authorization rules, it would destroy the reputations of their companies with their clients who have trusted the quality of the Hikvision products, and require complete overhauls of clients’ security systems at substantial consumer cost.¹⁶¹

The Commission’s proposed regulatory regime also threatens both jobs and safety. Hikvision creates many jobs for Americans, ranging from its own U.S.-based employees to those

¹⁵⁸ See, e.g., Blue Sky Technologies Comments; Guardian Safe & Lock Comments; Pittman Comments.

¹⁵⁹ See, e.g., Comments of Alpine Communications Inc., ET Docket No. 21-232 (filed Aug. 30, 2021) (stating that Hikvision’s products are “far superior to much of the market and allow [Alpine’s] customers to enjoy a quality product at an affordable price”); Gold Comments (describing how the quality and price of Hikvision cameras are superior to those of other manufacturers); Comments of John Prindle, ET Docket No. 21-232 (filed Aug. 20, 2021).

¹⁶⁰ See, e.g., Zuckerman Comments (“I feel if this is passed that there will be a lot of harm done to smaller contractors and installers that could and will impact our economy and the jobs market.”); Junto Technology Comments; Pittman Comments.

¹⁶¹ See, e.g., Junto Technology Comments (stating that a Hikvision equipment ban “will result in a major disruption to [its] business, loss of trust in [its] company”); Guardian Safe & Lock Comments; Gold Comments; Cortes Comments; Oakley Comments.

who distribute and install its products.¹⁶² And, as noted above, the security companies that rely on Hikvision products also provide jobs that would be placed at risk by the proposals of the NPRM. At the same time, the NPRM raises safety risks because the elimination of a quality yet affordable video surveillance manufacturer from the market may make new installations unaffordable to many homeowners, businesses, and organizations. As a result, schools, hospitals, community organizations, businesses, and residential properties will be able to deploy fewer cameras and receive less video coverage, which could result in more crimes perpetrated and a decrease in public safety.¹⁶³

Further, the Commission’s proposed equipment authorization rules for devices that receive authorization through the SDoC would adversely impact global trade commitments.¹⁶⁴ It would also disrupt and impose substantial burdens on manufacturers across the supply chain, affecting more than the covered entities.

Small business owners who rely on the sale of Hikvision video surveillance equipment have expressed concern over the political—rather than genuine national security—motivation behind the Commission’s proposed regulations.¹⁶⁵ It is imperative that the Commission recognizes that its proposed equipment authorization rules will go beyond mere posturing to

¹⁶² *See, e.g.*, Junto Technology Comments (stating that a Hikvision equipment ban would force the company “to cut [its] workforce in half and possibly shut down this division of [its] company”); Zuckerman Comments; Pittman Comments; Gold Comments.

¹⁶³ *See* Gold Comments.

¹⁶⁴ *See* Letter from Megan L. Brown, Counsel for CTA, to Marlene H. Dortch, Secretary, FCC, EA Docket No. 21-233, at 2 (filed June 11, 2021).

¹⁶⁵ *See, e.g.*, Folger Comments (“This feels like a political stunt . . .”); Brooks Comments (“Please punish China some other way.”); Hall Comments; Comments of Jason Walsh & Marian Bassalious, ET Docket No. 21-232 (filed Aug. 30, 2021).

directly impact the livelihoods of the American businesses and consumers that the Commission seeks to protect.

V. THE PROPOSED REGULATIONS WOULD VIOLATE THE CONSTITUTION’S EQUAL PROTECTION GUARANTEE.

The Commission’s proposed regulations unconstitutionally withhold equipment authorizations from otherwise-compliant products solely because they are manufactured by specific companies with foreign affiliations. The Equal Protection Clause of the Fourteenth Amendment—which applies to the federal government as well as the states¹⁶⁶—prohibits the government from “deny[ing] to any person within its jurisdiction the equal protection of the laws.”¹⁶⁷ The protections of the Fourteenth Amendment apply to foreign and alien corporations like Hikvision,¹⁶⁸ and corporations may assert equal protection for discrimination against their owners based on a suspect classification.¹⁶⁹ The Commission’s proposed regulations would violate those constitutional protections because they target Hikvision because it is Chinese—or more specifically, because its owners include a Chinese state-owned corporation.

A. The Commission’s Proposal Targets Manufacturers for Disparate Treatment Because of Their National Origin.

¹⁶⁶ *United States v. Ayala-Bello*, 995 F.3d 710, 714 (9th Cir. 2021) (“[T]he Supreme Court has extended the [Fourteenth Amendment’s] equal protection guarantee to bind the federal government too.”); *Pollack v. Duff*, 793 F.3d 34, 45 (D.C. Cir. 2015) (“[T]he principle of equal protection indisputably applies to the federal government as well as the states.”).

¹⁶⁷ U.S. Const. amend. XIV, § 1.

¹⁶⁸ *Disconton Gesellschaft v. Umbreit*, 208 U.S. 570, 579–580 (1908).

¹⁶⁹ *See, e.g., Carnell Const. Corp. v. Danville Redevelopment & Housing Auth.*, 745 F.3d 703, 714 (4th Cir. 2014) (collecting cases for the proposition that corporations may bring race-discrimination claims); *cf. Hudson Valley Freedom Theater, Inc. v. Heimbach*, 671 F.2d 702, 706 (2d Cir. 1982) (noting that Supreme Court precedent implicitly supports “[t]he principle that a corporation may assert equal protection claims when it alleges discrimination because of the color of its stockholders”).

The Commission targets Hikvision and other companies because they are “covered telecommunications equipment” manufacturers.¹⁷⁰ And those companies are covered manufacturers for only one reason: they are Chinese. The NDAA—which the Covered List and current proposed rules depend on¹⁷¹—defines “covered telecommunications equipment or services” as any equipment manufactured by, *inter alia*, Hikvision,¹⁷² or any entity “owned or controlled by, or *otherwise connected to*, the government of a covered foreign country,”¹⁷³ where “covered foreign country” is defined solely as “the People’s Republic of China.”¹⁷⁴ Thus, the Commission has chosen to place Hikvision on unequal footing in the private market based solely on a definition that is explicitly tied to Hikvision’s status as a Chinese company run by Chinese nationals.¹⁷⁵

A regulation that “classifies a person or group by race, alienage, or national origin” is “subject to strict scrutiny review, and will be sustained only if [it] is narrowly tailored to serve a compelling governmental interest.”¹⁷⁶ In the past, the Court has struck down laws that—like the

¹⁷⁰ *Covered Equipment NPRM* ¶ 8.

¹⁷¹ *Id.*

¹⁷² 2019 NDAA § 889(f)(3)(B).

¹⁷³ *Id.* § 889(f)(3)(D) (emphasis added).

¹⁷⁴ *Id.* § 889(f)(2). Because any manufacturer “connected to” the Chinese government is a “covered manufacturer,” Hikvision would fall under the Commission’s regulations based solely on its country of origin, whether or not it was also specifically defined as a covered manufacturer.

¹⁷⁵ Of course, a corporation’s place of incorporation is not necessarily the same thing as the national origin of its owners. *See, e.g., Bibliotechnical Athenaeum v. Am. Univ. of Beirut*, No. 20-cv-4068, 2021 WL 1061994, at *5 (S.D.N.Y. Mar. 19, 2021). But here, it is clear that Congress and the Commission have not identified Hikvision simply because it is *incorporated* in China, but because its ownership includes a state-owned corporation.

¹⁷⁶ *United States v. Lawson*, 677 F.3d 629, 637 (4th Cir. 2012). Although a limited category of restrictions on non-citizens or aliens—namely, participating in governmental functions such as serving as a police officer or teaching at a public school—is subject to rational basis

Commission’s proposed regulations—restricted commercial activities on the basis of national origin or alienage. In *Yick Wo v. Hopkins*, the Court sustained an as-applied challenge to a San Francisco ordinance that gave the city unlimited discretion to deny someone the ability to operate a laundry, when it was applied solely to Chinese nationals.¹⁷⁷ And in *Takahashi v. Fish and Game Commission*, the Court invalidated a California law that prevented anyone ineligible to become a U.S. citizen from obtaining a commercial fishing license.¹⁷⁸ Notably, under U.S. immigration law at the time, Japanese nationals were not eligible to become citizens, and an earlier draft of the California law applied expressly, and only, to Japanese citizens.¹⁷⁹

The Commission’s regulations achieve the same effect: denying a foreign entity the ability to engage in commercial activity because of its foreign origin.¹⁸⁰ Although promoting national security—the Commission’s stated goal here—can be a compelling interest, even laws intended to protect national security must be narrowly tailored if they are to survive strict scrutiny.¹⁸¹

review, the Court has been clear that “[t]he distinction between citizens and aliens . . . [is] ordinarily irrelevant to private activity.” *Ambach v. Norwick*, 441 U.S. 68, 74–75 (1979).

¹⁷⁷ 118 U.S. 356, 366, 374 (1886).

¹⁷⁸ 334 U.S. 410, 418–420 (1948).

¹⁷⁹ *Id.* at 412–13.

¹⁸⁰ The facially neutral category of “covered telecommunications equipment” does make this distinction any less pernicious, just as the facially neutral criterion of eligibility for U.S. citizenship did not save the ordinance in *Takahashi*. *See id.* at 413 (noting that earlier version of ordinance “prohibited issuance of a license to any ‘alien Japanese’” but that that language was amended “for fear that it might be ‘declared unconstitutional’”).

¹⁸¹ *See, e.g., Twitter, Inc. v. Sessions*, 263 F. Supp. 3d 803, 816 (N.D. Cal. 2017) (holding, in First Amendment context, that government restriction on a company disclosing the number of national security letters it received failed strict scrutiny where restriction was not narrowly tailored).

The decision in *Twitter v. Sessions* is instructive. In that case, Twitter sought to publish a “transparency report” detailing the aggregate number of national security letters it had received pursuant to the Foreign Intelligence Surveillance Act.¹⁸² The government denied the request because the Twitter report was inconsistent with the government’s approved framework.¹⁸³ Holding that the government’s denial was a prior restraint on speech, the court applied strict scrutiny¹⁸⁴ and held that the government had not demonstrated that its action was “narrowly tailored to prevent a national security risk of sufficient gravity to justify restraint.”¹⁸⁵ Specifically, the government did not indicate that its decision “reflected any narrow tailoring . . . to take into consideration . . . the nature of the provider, the volume of any requests involved or the number of users on the platform.”¹⁸⁶ Instead, the government relied on “a generic, and seemingly boilerplate, description of mosaic theory and a broad brush concern that the information at issue will make more difficult the complications associated with intelligence gathering in the internet age.”¹⁸⁷

The Commission’s reasoning suffers from the same defects: The NPRM does not reflect any narrow tailoring to account for *actual* security concerns, if any, posed by Hikvision’s specific products. On the contrary, it sweeps extraordinarily broadly, effectively banning a manufacturer from selling any products based solely on the manufacturer’s national origin.

¹⁸² *Id.* at 806.

¹⁸³ *Id.* at 806–07.

¹⁸⁴ *Id.* at 815.

¹⁸⁵ *Id.* at 816.

¹⁸⁶ *Id.* at 816–17.

¹⁸⁷ *Id.* at 817. In a subsequent decision, after a more complete record was developed, the court held that the government’s position satisfied strict scrutiny. *See Twitter, Inc. v. Barr*, 445 F. Supp. 3d 295, 303 (N.D. Cal. 2020).

There are many less restrictive alternatives that would further the Commission’s stated goals, as explained above.

The fact that Congress authorized the Commission to compile a list of covered manufacturers does not provide a basis for the Commission to single out covered manufacturers for disparate treatment. While requiring the Commission to maintain a list of covered manufacturers, Congress certainly has not instructed the Commission to use that list as a basis to deny a class of manufacturers the ability to import their products into the United States. Moreover, even if Congress *had* purported to instruct the Commission to deny all covered providers equipment authorizations, that instruction would be equally constitutionally suspect—Congress may not contravene the Equal Protection Clause any more than the Commission acting alone.

Nor does the fact that Congress prohibited *government* use of covered equipment justify the Commission’s decision to effectively ban covered equipment from the private market, because the Equal Protection Clause is more permissive of restrictions on foreign participation in government activity than private activity.¹⁸⁸

At the same time, the proposed rules are wildly underinclusive—another sign that they are not narrowly tailored.¹⁸⁹ Because the Commission’s proposed regime targets only Chinese companies, it entirely ignores companies from every other country on earth that might pose equal or far greater national security risks. A scheme that entirely bars a Chinese manufacturer from

¹⁸⁸ *Ambach*, 441 U.S. at 74–75.

¹⁸⁹ *See, e.g., Ark. Writers’ Project, Inc. v. Ragland*, 481 U.S. 221, 232 (1987) (statutory scheme was not “narrowly tailored to achieve [its] end” because it was “both overinclusive and underinclusive”).

the U.S. market while imposing no restrictions on companies from Russia, Iran, or North Korea is not narrowly tailored.

B. The Commission’s Regulations Cannot Survive Even Rational Basis Review, Because They Are Based on Irrational Logical Leaps.

Even if the Commission’s proposed rules were not subject to heightened review, the regulations would still be unconstitutional because even under rational basis review—the most relaxed constitutional standard—a regulation cannot “be enacted for arbitrary or improper purposes.”¹⁹⁰ The regulation must be “rationally related to legitimate government interests,”¹⁹¹ and “must rest upon some ground of difference having a fair and substantial relation to the object of the legislation, so that all persons similarly circumstanced shall be treated alike.”¹⁹² Moreover, while government regulation is not subject to courtroom standards of factfinding, it must still be supported by, at least, “*rational* speculation.”¹⁹³

But the Commission’s logic here—that *every* consumer product manufactured by certain manufacturers poses a national security threat simply by virtue of *who made it*, without any regard to its actual capabilities or how it is used, and without imposing any restrictions on functionally identical products by other manufacturers—exceeds even the generous limits of rational-basis review. Indeed, to speculate that there is *no scenario* in which a product can be safely deployed by a private user simply because the manufacturer is affiliated with a foreign government appears to be the kind of logical leap that is the height of *irrational* speculation. A

¹⁹⁰ *Golinski v. U.S. Office of Personnel Mgmt.*, 824 F. Supp. 2d 968, 996 (E.D. Cal. 2012).

¹⁹¹ *Doe v. Mich. Dep’t of State Police*, 490 F.3d 491, 501 (6th Cir. 2007) (quoting *Washington v. Glucksberg*, 521 U.S. 702, 728 (1997)).

¹⁹² *Johnson v. Robinson*, 415 U.S. 361, 374–75 (1974) (quoting *F.S. Royster Guano Co. v. Virginia*, 253 U.S. 412, 415 (1920)).

¹⁹³ *Heller v. Doe by Doe*, 509 U.S. 312, 320 (1993) (emphasis added) (quoting *FCC v. Beach Commc’ns, Inc.*, 508 U.S. 307, 315 (1993)).

law that discriminates between entities based solely on an irrational conclusion is unconstitutional.

Because there is no rational basis—much less a narrowly tailored one—for concluding that Chinese manufacturers’ products categorically cannot be safely deployed under any circumstances in private companies’ security systems, the Commission’s proposed regulations deny Hikvision equal protection, and are constitutionally invalid.

VI. THE COMMISSION’S STRUCTURE MAY VIOLATE THE APPOINTMENTS CLAUSE.

Because the FCC Commissioners are appointed by the President and wield significant powers that are executive in nature, but are not removable at will by the President, their status may well conflict with the Constitution’s separation of powers. Although the Supreme Court in 1935 in *Humphrey’s Executor* held that the Federal Trade Commission, as a multimember, expert body, did not run afoul of the Appointments Clause,¹⁹⁴ it has not recently revisited the question. However it has at least raised the possibility that *Humphrey’s Executor* was wrongly decided.¹⁹⁵ Recent Supreme Court cases, including *Free Enterprise Fund v. Public Company Accounting Oversight Board*,¹⁹⁶ *Seila Law*,¹⁹⁷ and *Collins v. Yellen*,¹⁹⁸ make clear that the President must wield unhindered removal power over purely executive officers who wield substantial executive power: “At-will removal ensures that the lowest officers, the middle grade,

¹⁹⁴ *Humphrey’s Ex’r v. United States*, 295 U.S. 602, 631–632 (1935).

¹⁹⁵ *See Seila Law LLC v. Consumer Financial Protection Bureau*, 140 S. Ct. 2183, 2198 (2020) (quoting *Humphrey’s Ex’r*, 295 U.S. at 628) (“Rightly or wrongly, the Court viewed the FTC (as it existed in 1935) as exercising ‘no part of the executive power.’”).

¹⁹⁶ 561 U.S. 477 (2010).

¹⁹⁷ 140 S. Ct. 2183 (2020).

¹⁹⁸ 141 S. Ct. 1761 (2021).

and the highest, will depend, as they ought, on the President, and the President on the community.”¹⁹⁹ That is because from the moment “an officer is appointed, it is only the authority that can remove him, and not the authority that appointed him, that he must fear.”²⁰⁰ Were this same principle to be applied to multi-member agencies like the FCC, the Commission’s structure would be unconstitutional. Because the Commissioners would be unconstitutionally insulated from removal, they would lack constitutional authority to promulgate the NPRM’s proposed rules.

VII. CONCLUSION

The proposed rules cannot and should not be adopted. With respect to Hikvision, they will not further national security or end user cybersecurity, and they will harm the ability of end users’ businesses to secure their premises and personnel cost effectively. Hikvision cameras and NVRs are not telecommunications or internet network equipment, and are not critical infrastructure. Moreover, the Commission lacks any authority to utilize the equipment authorization process to promulgate this type of ban, which is wholly unrelated to the statutory purpose of equipment authorization, which is to protect against harmful RF interference. Adoption of these rules would be arbitrary, capricious, and contrary to both statutory law and the U.S. Constitution.

Respectfully submitted,



John T. Nakahata
Timothy J. Simeone

¹⁹⁹ *Collins*, 141 S. Ct. at 1784.

²⁰⁰ *Synar v. United States*, 626 F. Supp. 1374, 1401 (D.C. Cir. 1986).

Deepika Ravi
John Grimm
Annick Banoun
HARRIS, WILTSHIRE & GRANNIS LLP
1919 M Street, NW, Suite 800
Washington, DC 20036
(202) 730-1300
jnakahata@hwglaw.com

Counsel for Hikvision USA, Inc.

September 20, 2021